УДК 621.391.28

Мошак Н.Н., Россия, Санкт-Петербург, ГУТ им. проф. М.А.Бонч-Бруевича

Модели протоколов VPN в задаче анализа инфокоммуникационной сети

Moshak N.N.

VPN PROTOCOL MODELS IN ANALISYS TASK OF INFOCOMMUNICATION NETWORK

Использование технологии защищенных виртуальных сетей (Virtual Private Network - VPN) позволяет обеспечить криптозащиту информации в открытой сетевой среде, включая Интернет, при организации доступа пользователей к ресурсам локальной вычислительной сети (ЛВС) удаленных филиалов своих организаций и/или организации защищенных каналов связи или туннелей между защищенными ЛВС корпоративных сетей [Малюк, Зима].

Каждый выделенный виртуальный канал VPN формируется в компьютере пользователя или в пограничных маршрутизаторах входа в открытую сеть общего пользования с помощью механизмов тунелирования (инкапсуляции) базового примитива протокола логического уровня корпоративной сети в примитив защищенного протокола. VPN-агенты могут осуществлять функции шифрования/расшифрования, аутентификации, а также контроль целостности сообщения посредством электронной цифровой подписи (ЭЦП) или имитовставки (ИВ).

Как правило, VPN-агенты поддерживают несколько стандартных протоколов для организации защищенных туннелей, которые могут применяться на различных уровнях логической структуры эталонной модели архитектуры ВОС Международной организации МОС. Хотя указанные протоколы могут размещаться на всех уровнях эталонной модели к средствам VPN относят только те, которые полностью прозрачны для сетевых служб и приложений пользователя. Это протоколы защищенных туннелей канального, сетевого и транспортного уровней. Указанные три уровня, которые в терминах модели ВОС образуют логическую структуру транспортной системы (ТС) области взаимодействия открытых систем [Мошак], называют также VPN-уровнями. Логическую структуру ТС IP-сети образуют соответственно уровни TCP/UDP, IP и уровень сетевого интерфейса.

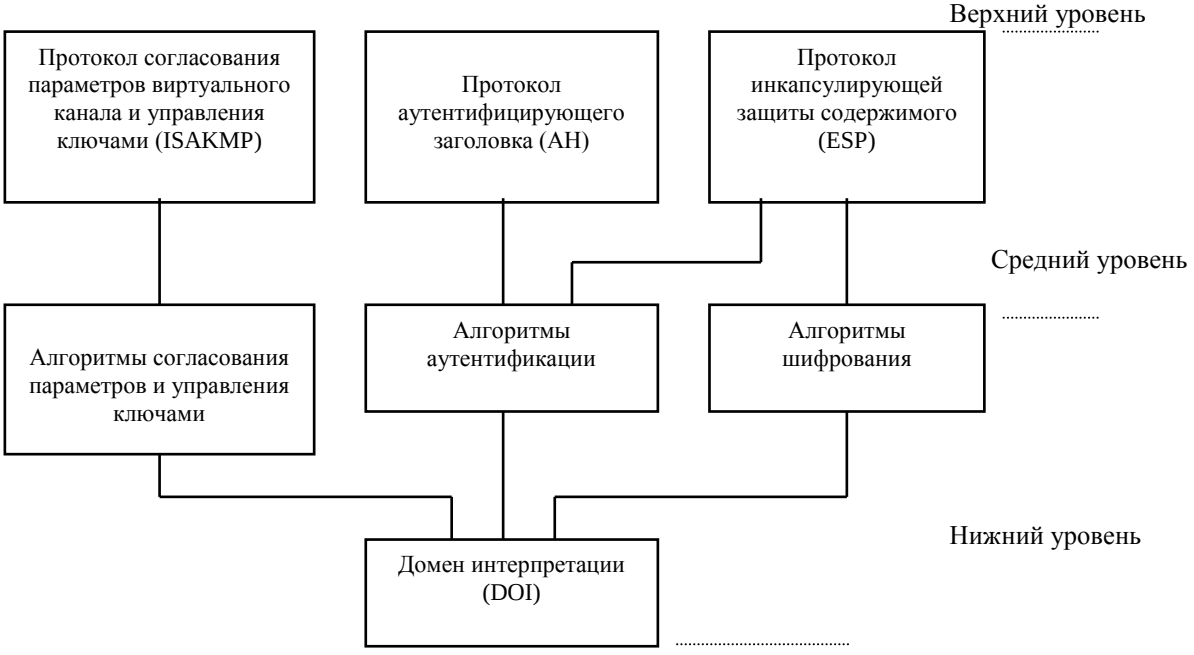


Рис. 1. Архитектура средств безопасности IPSec

Наиболее известным протоколом VPN, работающим над транспортным уровнем, стал протокол Secure Socket Layer (SSL) и его новая открытая реализация Transport Layer Security (TLS). Протоколом SSL/TLS могут воспользоваться любые приложения и любые протоколы прикладного уровня. Однако в приложениях должны быть встроены явные вызовы функций этого протокола. На сетевом и канальном уровнях зависимость приложений от протоколов VPN исчезает совсем. Однако здесь появляется проблема их зависимости от конкретной сетевой технологии. Например, проложить защищенный канал через гетерогенную среду с помощью единого протокола канального уровня невозможно.

Работающий на сетевом уровне протокол IPSec является компромиссным вариантом. С одной стороны, он прозрачен для приложений, а с другой — он может работать практически во всех сетях (и в том числе в рассматриваемой нами инфокоммуникационной сети) так как основан на широко распространенном протоколе IP: в настоящее время в мире только 1% компьютеров не поддерживает IP вообще, остальные 99% используют его либо как единственный протокол, либо в качестве одного из нескольких протоколов.

В соответствии с протоколом IPSec архитектура средств безопасности информационного обмена разделяется на три уровня (рис.1).

На верхнем уровне расположены следующие протоколы:

- **протокол** согласования параметров виртуального канала и управления ключами (Internet Security Association Key Management Protocol — ISAKMP), обеспечивающий общее управление защищенным виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации;

- **протокол** аутентифицирующего заголовка (Authentication Header — AH), предусматривающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;

- **протокол** инкапсулирующей защиты содержимого (Encapsulating Security Payload — ESP), обеспечивающий криптографическое закрытие передаваемых пакетов сообщений и предусматривающий также выполнение всех функций протокола аутентифицирующего заголовка AH. Протокол ESP может поддерживать функции шифрования и аутентификации/целостности в любых комбинациях, т. е. либо и ту и другую группу функций, либо только аутентификацию/целостность, либо только шифрование.

Использование в IPSec двух различных протоколов защиты виртуального канала (AH и ESP) обусловлено практикой, применяемой во многих странах на ограничение экспорта и/или импорта криптосредств. Каждый из этих протоколов может использоваться как самостоятельно, так и одновременно с другим.

Алгоритмы аутентификации и шифрования, используемые в протоколах AH и ESP, образуют **средний уровень** архитектуры IPSec. К этому уровню относятся также алгоритмы согласования параметров и управления ключами. В настоящий момент для протоколов AH и ESP зарегистрировано два алгоритма аутентификации — **HMAC-MD5** (Hashed Message Authentication Code - Message Digest version 5) и **HMAC-SHA1** (Hashed Message Authentication Code — Secure Hash Algorithm version 1). Данные алгоритмы являются алгоритмами **аутентификации с секретным ключом**. Если секретный ключ известен только передающей и принимающей сторонам, это обеспечит аутентификацию источника данных, а также целостность пакетов, пересылаемых между двумя сторонами. Алгоритмом, использующимся **по умолчанию**, определен алгоритм **HMAC-MD5.** Для протокола ESP зарегистрировано семь алгоритмов шифрования. Алгоритм шифрования DES (Data Encryption Standard), как и алгоритм HMAC-MD5, принят по умолчанию и необходим для обеспечения IPSec-совместимости. В качестве альтернативы DES определены алгоритмы Triple DES, CAST-128, RC5, IDEA, Blowfish и ARCFour [10].

Протоколы защиты виртуального канала верхнего уровня архитектуры IPSec (AH и

ESP) не зависят от конкретных криптографических алгоритмов. В них могут использоваться любые методы аутентификации, типы ключей (симметричные или несимметричные), алгоритмы шифрования и распределения ключей. Алгоритмическая независимость протоколов AH и ESP требует предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых взаимодействующими сторонами. Для согласования параметров виртуального канала и ***управления криптографическими ключами*** на сетевом уровне модели OSI наиболее широкое распространение получили такие протоколы, как SKIP (Simple Key management for Internet Protocols) и ISAKMP (Internet Security Association and Key Management Protocol). В четвертой версии протокола Ipv4 может применяться как протокол ISAKMP, так и протокол SKIP, а протокола IPv6 – только протокол ISAKMP. Протокол согласования параметров виртуального канала и управления ключами **ISAKMP обеспечивает** общее управление защищенным виртуальным соединением, включая **согласование используемых алгоритмов криптозащиты,** а также **генерацию и распределение ключевой информации.** В сравнении с протоколом SKIP протокол ISAKMP более сложен в реализации, но обеспечивает повышенную безопасность информационного взаимодействия. В соответствии с протоколом ISAKMP при формировании защищенного виртуального канала взаимодействующие стороны должны выработать, общий контекст безопасности (Security Association — SA) и только затем использовать элементы этого контекста, такие как алгоритмы и ключи. Протокол ISAKMP описывает базовые процедуры аутентификации сторон, обмена ключами и согласования всех остальных параметров защищенного IPSec-туннеля. Однако **ISAKMP не содержит конкретные алгоритмы обмена криптографическими ключами**. Поэтому для обмена ключами могут использоваться другие протоколы. В спецификации IPSec в качестве такого протокола, используемого при формировании общего защищенного туннеля, выбран **протокол Oakley, основанный на алгоритме Диффи-Хеллмана**. Объединение протоколов ISAKMP и Oakley обозначают как **ISAKMP/Oakley**. Следует отметить, что протоколы ISAKMP и Oakley разработаны таким образом, что они не зависят от спецификации IPSec. Например, для повышения безопасности процесса установления сеансов протокол Oakley вполне можно использовать вместе с протоколом SSL (Secure Sockets Layer).

Архитектура IPSec является полностью открытой. В IPSec могут использоваться протоколы и алгоритмы, которые изначально не разрабатывались для этой архитектуры. Поэтому возникла необходимость в так называемом домене интерпретации (Domain of Interpretation, DOI), который обеспечивал бы совместную работу всех включаемых протоколов и алгоритмов. Домен интерпретации DOI играет роль фундамента в архитектуре IPSec и является, по сути, **базой данных**, **хранящей сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т.д.**

Протокол ISAKMP предусматривает не только защиту от нарушений конфиденциальности и подлинности согласовываемых глобальных параметров, но и защиту от повтора, задержек и удаления защищенных сообщений. Для защиты от перечисленных атак применяются так называемые идентифицирующие цепочки. Эти цепочки формируются инициатором и его партнером с использованием текущего времени и присутствуют во всех ISAKMP-сообщениях. **Для передачи ISAKMP-сообщений** может использоваться любой протокол, однако в спецификации IPSec в качестве такого протокола определен **протокол UDP с номером порта 500**. Формат и структура заголовка ISAKMP-сообщения приведен на рисунке 2.

Идентифицирующая цепочка инициатора
Идентифицирующая цепочка партнера

След. заголовок	Номер версии	Тип обмена	Флаги
Индикатор сообщения			
Длина			

Рисунок 2. - Формат заголовка ISAKMP-сообщения

Исключением является первый запрос на формирование защищенного канала, в который включена только одна из идентифицирующих цепочек – цепочка инициатора. Как инициатор, так и партнер для каждого отправляемого сообщения генерирует на основе текущего времени свою идентифицирующую цепочку и вставляет ее в это сообщение. В каждое ответное сообщение помимо идентифицирующей цепочки отправителя вставляется также цепочка противоположной стороны, полученная в сообщении, для которого формируется этот ответ. При получении ответного сообщения получатель проверяет наличие посланной им идентифицирующей цепочки. При задании максимального времени следования ожидаемого сообщения использование идентифицирующих цепочек позволяет обнаружить повторные, задержанные и удаленные сообщения.

Протокол **SKIP** проще в реализации, но он, в отличие от протокола ISAKMP, **не поддерживает переговоров по поводу алгоритмов шифрования**. Для согласования используемых алгоритмов шифрования используется протокол ICMP (Internet Control Message Protocol, RFC 792), который осуществляет аутентификацию согласовываемых параметров. Для защиты от приема ложной информации в заголовок каждого SKIP-пакета, содержащего передаваемый ICMP-пакет, помещается имитовставка. **С целью** безопасного **распределения открытых ключей**, исключающего нарушение их целостности и подлинности, предлагается **использовать цифровые сертификаты, соответствующие стандарту X.509**.

Реализация **SKIP**, устанавливаемая непосредственно **над IP-драйвером**, обрабатывает весь трафик, не накладывая никаких ограничений ни на вышележащее программное обеспечение, ни на физические каналы, используемые для передачи информации. Процедура формирования зашифрованного пакета с применением протокола SKIP приведена на рис. 3.

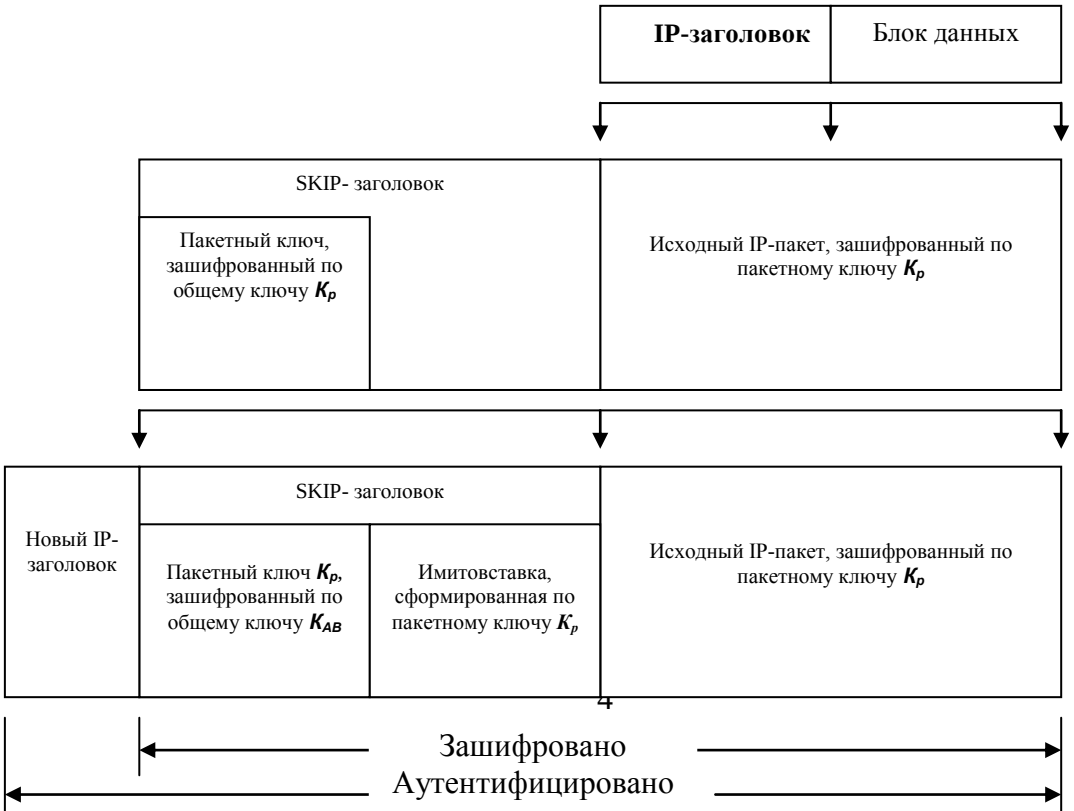


Рис. 3. Процедура формирования зашифрованного пакета с применением протокола SKIP

Приведем алгоритм формирования зашифрованного пакета с применением протокола SKIP.

1. Исходный IP-пакет зашифровывается по пакетному ключу K_p и инкапсулируется в SKIP-пакет.

2. Пакетный ключ K_p зашифровывается по общему секретному ключу K_{AB} и помещается в SKIP-заголовок, при этом в SKIP-заголовке резервируется поле под эталонную характеристику результирующего IP-пакета.

3. Полученный SKIP-пакет инкапсулируется в результирующий IP-пакет.

4. Для результирующего IP-пакета с помощью хэш-функции рассчитывается по пакетному ключу K_p эталонная характеристика и полученное значение помещается как имитовставка в зарезервированное поле SKIP-заголовка.

Таким образом, протокол SKIP помимо эффективного распределения ключей обеспечивает аутентификацию и криптографическое закрытие IP-пакетов. Поскольку пакетный ключ K_p зашифрован по общему секретному K_{AB} расшифровать этот пакетный ключ смогут только отправитель и получатель. Тем самым исключается возможность подмены имитовставки и расшифровывания исходного IP-пакета. Структура пакета SKIP приведена на рис.4.

Ver	svd	Source NSID	Dest NSID	NEXT HEADER
Counter n				
K_{AB} Alg	Crypt Alg		MAC Alg	Comp Alg
K_p encrypted in K_{AB} (typically 8-16 bytes)				
Source Master Key-ID (If Source NSID is non-zero)				
Destination Master Key-ID (If Dest NSID is non-zero)				

Рис.4. Структура пакета SKIP.

Режимы инкапсуляции (туннелирования) и шифрования могут применяться как совместно, так и раздельно. Структура SKIP-пакета, получающегося в результате такой инкапсуляции, показана на рис.5. Если применяется режим только аутентификации или только инкапсуляции, заголовки AH и ESP, ответственные за аутентификацию и инкапсуляцию, могут изыматься из пакета.

IP	SKIP	AH	ESP	Inner protocol

Рис.5.Структура пакета SKIP

Шифрование с инкапсуляцией (его называют также туннелированием) подразумевает, что весь исходный IP-пакет шифруется и помещается в поле данных нового SKIP-пакета. При этом может производиться также и замена адресов получателя-отправителя в заголовке пакета. Такую замену называют ***векторизацией*.**

Протоколы AH и ESP поддерживают работу в двух режимах:

Туннельный режим. IP-пакеты защищаются целиком, включая заголовки. Он

является основным режимом. При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищенном виде в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют **на специально выделенных защитных шлюзах**, в роли которых могут выступать **маршрутизаторы или межсетевые экраны. Между такими шлюзами и формируются защищенные туннели IPSec.** Туннелирование IP-пакетов полностью прозрачно для оконечных пользователей. На оконечных системах туннельный режим может использоваться для поддержки удаленных и мобильных пользователей. В этом случае на компьютерах этих пользователей должно быть установлено программное обеспечение, реализующее туннельный режим IPSec.

В транспортном режиме в конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок. Соответственно **в транспортном режиме заголовок IPSec размещается между сетевым (IP) и транспортным (TCP или UDP)** заголовками обычного IP-пакета. Транспортный режим быстрее туннельного и разработан для применения **на оконечных системах**. Данный режим может использоваться для поддержки удаленных и мобильных пользователей, а также защиты информационных потоков внутри локальных сетей.

Туннель IPSec между двумя локальными сетями **может поддерживать множество индивидуальных каналов передачи данных**, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования по сравнению с технологией второго уровня. В соответствии с архитектурой средств безопасности формационного обмена IPSec разделяется на три уровня (рис. 1).

Протокол заголовка аутентификации AH (Authentication Header) [RFC1826], [RFC1827] предусматривает аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений. Параметры аутентификации рассчитываются с использованием всех полей дейтаграммы IP (включая не только заголовок IP, но и заголовки других протоколов, а также пользовательские данные), которые не могут изменяться в процессе доставки. Поля или опции, которые при доставке изменяются (например, счетчик интервалов, время жизни, идентификаторы, смещения фрагмента или указатели маршрутов) при расчете не принимаются во внимание (предполагается, что они имеют нулевые значения). Формат заголовка AH показан на рис.2.

Следующий заголовок	Размер	Резерв (0)
Параметры безопасности SPI		
Номер последовательности		
Данные аутентификации		

Рис.2. Формат заголовка AH

Next Header - следующий заголовок после поля данных аутентификации). ***Size*** - размер поля данных аутентификации), ***Security Parameters Index (SPI)*** указывает параметры безопасности для дейтаграммы, номер последовательности - используется для защиты от ложного воспроизведения пакетов), ***Authentication Data*** - данные аутентификации или хэш-код в виде переменного числа 32-битовых слов (для MD5 размер хэш-кода равен 16 байтам).

Протокол инкапсулирующей защиты содержимого (IP Encapsulating Security Payload — ESP) [RFC1826], [RFC1827] обеспечивает криптографическое закрытие передаваемых пакетов сообщений и предусматривающий также выполнение всех функций протокола AH. В зависимости от пользовательских требований к безопасности этот механизм может применяться для шифрования сегментов транспортного уровня (например, TCP, UDP, ICMP, IGMP) или дейтаграмм IP целиком. Чтобы обеспечить конфиденциальность всей исходной дейтаграммы требуется использовать инкапсуляцию. Формат заголовка ESP показан на рис.3.

Параметры безопасности SPI	
Номер последовательности	
Данные	
	Заполнитель (0-255байт)
Длина заполнителя	Следующий заголовок
Данные аутентификации	

Рис.3. Формат заголовка ESP

Security association identifier SPI - 32-битовое псевдослучайное значение, идентифицирующее ассоциации безопасности дейтаграммы. Если ассоциаций не создано, поле SPI содержит значение 0x00000000. Поле SPI подобно параметру SAID, используется другими протоколами безопасности. Заполнитель (Для поддержания кратности поля данных 4 байтам и частичной конфиденциальности трафика).

Протоколы аутентифицирующего заголовка AH и инкапсулирующей защиты содержимого ESP поддерживают работу в двух режимах: туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки и транспортном, обеспечивающим полную защиту только содержимого IP-пакетов. В транспортном режиме передача IP-пакета через сеть выполняется с помощью оригинального заголовка. В туннельном режиме исходный пакет помещается в новый IP-пакет. Заголовки протокольных блоков AH и ESP располагаются в транспортном режиме после заголовка исходного IP-пакета и перед заголовками протоколов верхних уровней, а в туннельном режиме – после заголовка внешнего IP-пакета и перед заголовком внутреннего исходного IP-пакета (рис.4).

Транспортный режим	Туннельный режим
[IPисх.][AH][верх.]	[IPвнеш.][AH][IPисх.][верх.]]
[IPисх][ESP][верх.]	[Ipвнеш.][ESP][IPисх.][верх.]]
[IPисх.][AH][ESP][верх.]	

Рис.4. Расположение полей заголовков протокольных блоков в транспортном и туннельном режимах

Таблица 1. - Сравнение различных режимов работы для протоколов AH и ESP

Протокол	Транспортный режим	Туннельный режим
AH	Идентифицирует протокол-пассажир IP, а также отдельные части заголовка IP и заголовка рассширений IPv6	Идентифицирует весь внутренний пакет IP (заголовок и протокол-пассажир внутреннего пакета IP), а также отдельные части внешнего заголовка IP и внешних заголовков расширений IPv6
ESP	Шифрует протокол-пассажир IP и все заголовки рассширений IPv6, следующие за заголовком ESP	Шифрует внутренний пакет IP
ESP с аутентификацией	Шифрует протокол-пассажир IP и все заголовки рассширений Ipv6, следующие за заголовком ESP. Идентифицирует протокол-пассажир IP и заголовок IP.	Шифрует внутренний пакет IP. Идентифицирует внутренний пакет IP.

Сравнение различных режимов работы для протоколов AH и ESP представлено в таблице 1.

Приведем алгоритм работы протокола IPSec:

1. по адресу IP получателя выбрать алгоритм шифрования, ЭЦП (ИВЗ) и криптографические ключи. Если адрес получателя имеется в настройках, то перейти к п.2;

2. сгенерировать ЭЦП или вычислить ИВ и **добавить в пакет;**

3**. зашифровать пакет на симметричном ключе;**

4**. сформировать заголовок VPN**-агента и **инкапсулировать** зашифрованный пакет;

5**. отправить** пакет VPN-агенту;

6. при получении пакета **аутентифицировать отправителя** по его адресу. Если адрес имеется в списке разрешенных и пакет не поврежден, то перейти к п.7;

7. выбрать алгоритм шифрования, ЭЦП и криптографические ключи;

8. **расшифровать** пакет и **проверить целостность (ЭЦП или ИЗВ)**. Если целостность не нарушена, то перейти к п.9;

9. **отправить** исходный пакет в защищенный сегмент корпоративной ЛВС

получателю.

Протокол аутентифицирующего заголовка (AH)

Протокол аутентифицирующего заголовка (Authentication Header — AH) **обеспечивает целостность** IP-пакетов **и аутентификацию источника данных**, а также **защиту от воспроизведения** ранее посланных IP-пакетов. Этот протокол полностью защищает от подлога и случайного искажения содержимое IP-пакетов, включая данные протоколов более высоких уровней.

В основе обеспечения целостности и аутентификации данных лежит один из приемов шифрования — шифрование с помощью односторонней функции (one-way function), называемой также хэш-функцией (hash function) или дайджест-функцией (digest function).

Эта функция, примененная к шифруемым данным, дает в результате значение-дайджест, состоящее из фиксированного небольшого числа байт. Дайджест передается в IP-пакете вместе с исходным сообщением. Получатель, зная, какая односторонняя функция шифрования была применена для составления дайджеста, заново вычисляет его, используя исходное сообщение. Если значения полученного и вычисленного дайджестов совпадают, это значит, что содержимое пакета во время передачи не было подвергнуто никаким изменениям. Знание дайджеста не дает возможности восстановить исходное сообщение и поэтому не может быть использовано для защиты, но зато оно позволяет проверить целостность данных.

Дайджест является своего рода контрольной суммой для исходного сообщения. Однако имеется и существенное отличие. Использование контрольной суммы — это средство проверки целостности передаваемых сообщений по ненадежным линиям связи, и оно не направлено на борьбу со злонамеренными действиями. Ведь, наличие контрольной суммы в передаваемом пакете не помешает злоумышленнику подменить исходное сообщение, добавив к нему новое значение контрольной суммы. **В отличие от контрольной суммы при вычислении дайджеста используется секретный ключ**. Если для получения дайджеста применялась односторонняя функция с параметром (в качестве которого выступает секретный ключ), известным только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

Полнота защиты полей IP-заголовков зависит от используемою режима работы - туннельного или транспортного.

Использование AH в туннельном режиме

В туннельном режиме защищаются все поля IP-заголовков. Каждый обычный IP-пакет помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля.

Рис. 5. Протокол AH в туннельном режиме.

3.1.2 Использование AH в транспортном режиме

При использовании протокола AH в транспортном режиме защита не накладывается лишь на те поля IP-заголовков, которые меняются на маршруте доставки непредсказуемым образом. К таким полям для протокола IPv4 относится поле Time to Live, задающее время жизни IP-пакета, а также поле Type of Service, определяющее тип его обслуживания. В транспортном режиме в конверт IPSec помещается только содержимое защищаемого IP-пакета и к полученному конверту добавляется исходный IP-заголовок.

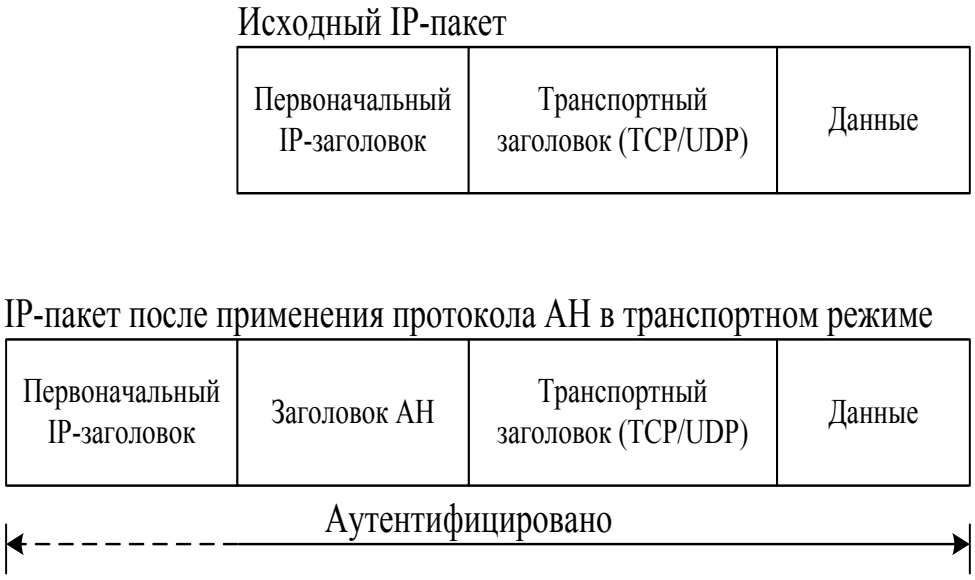


Рис. 6. Протокол AH в транспортно режиме.

Формат заголовка представлен на рисунке

Next Header	Payload Len	Зарезервировано
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (переменная длина)		

Рис. 7. Формат заголовка AH.

Next Header — однобайтовое поле, содержащее код типа следующего заголовка, вложенного в IPSec-пакет. Например, если в IPSec-пакете содержится TCP-пакет, то данное поле будет содержать число 6 — код протокола TCP.

Payload Len — длина заголовка AH в 32-битных словах минус 2.

SPI — 32-битный индекс параметров безопасности, определяющий структуру SA (Security Association), содержащую все параметры туннеля IPSec, включая типы криптографических алгоритмов и ключи шифрования.

Sequence Number — беззнаковое 32-битное целое, увеличиваемое на единицу после передачи каждого защищенного по протоколу AH IP-пакета. Данное поле обеспечивает защиту от воспроизведения ранее посланных IP-пакетов. Отправитель обязан поддерживать этот счетчик. При формировании каждого защищенного сеанса информационного обмена в рамках туннеля IPSec обе взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их.

Authentication Data — поле переменной длины, содержащее информацию, используемую для аутентификации пакета и называемую MAC-кодом (Message Authentication Code). Это поле называют также цифровой подписью, имитовставкой, хэш-значением или криптографической контрольной суммой (Integrity Check Value — ICV) пакета. Способ вычисления этого поля определяется алгоритмом аутентификации.

Для вычисления содержимого поля Authentication Data могут применяться различные алгоритмы. В настоящее время предписывается обязательная поддержка **алгоритмов HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций (дайджест-функций) с секретными ключами**. Секретные ключи генерируются в соответствии с протоколом ISAKMP.

Таким образом, независимо от режима работы, протокол AH предоставляет меры защиты от атак, ориентированных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Несмотря на нахождение IP-заголовков за пределами защищенного IPSec-конверта, **протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов.** Но следует иметь в виду, что аутентификация по протоколу AH не допускает манипулирование основными полями IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов (Network Address Translation — NAT), так как манипулирование IP-заголовками необходимо для его работы.

Протокол инкапсулирующей защиты содержимого (ESP).

Протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload — ESP) обеспечивает выполнение следующих функций по защите информационного обмена:

- **криптографическое закрытие** содержимого IP-пакетов;
- частичная защита **от анализа трафика** путем применения **туннельного режима**;
- формирование и проверка цифровой подписи IP-пакетов для их защиты от нарушений **подлинности** и **целостности**;
- защита **от воспроизведения** IP-пакетов.

Представленный перечень функций по защите информационного обмена показывает, что функциональность протокола ESP шире, чем у протокола AH. Протокол ESP обеспечивает конфиденциальность данных, а также поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения. Обобщенно все функции защиты, поддерживаемые протоколом ESP, можно свести к аутентификации, которую обеспечивает также протокол AH, и криптографическому закрытию передаваемых IP-пакетов. Спецификация IPSec допускает использование протокола ESP для криптографического закрытия IP-пакетов без использования функций аутентификации. Кроме того, допускается использование фиктивного шифрования при выполнении функций протокола AH. Таким образом, в

протоколе ESP функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов (Network Address Translation — NAT), поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать.

Независимо от режима использования протокола ESP его заголовок формируется как инкапсулирующая оболочка для зашифрованного содержимого.

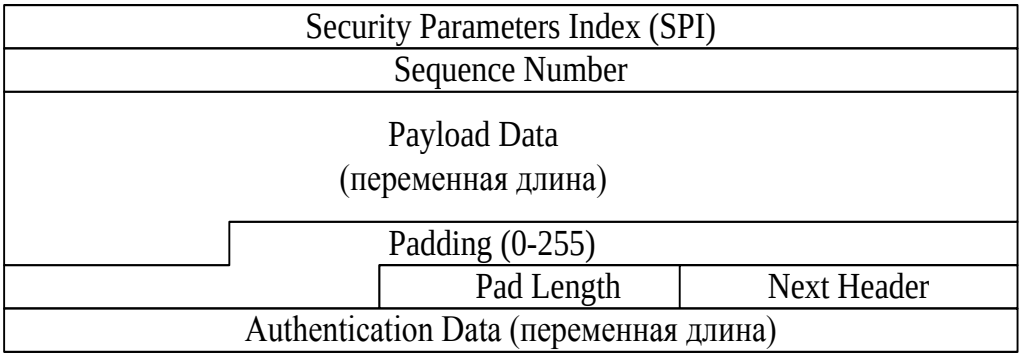


Рис. 8. Формат заголовка ESP.

Поля SPI, Sequence Number, Next Header и Authentication Data имеют тот же смысл, что и для AH. Поле Authentication Data помещается в заголовок ESP только при включенной аутентификации. В поле Payload Data, имеющее переменную длину, включается инкапсулируемый пакет, который шифруется вместе с полями Padding, Pad Length и Next Header. Поле Padding представляет собой байты, добавляемые для обеспечения кратности длины инкапсулируемого пакета и размера блока алгоритма шифрования. Поле Pad Length содержит длину области Padding. В туннельном режиме использования протокола ESP в качестве инкапсулируемого пакета выступает весь исходный IP-пакет (рис. 3.13), а в транспортном — только его содержимое, т. е. исходный TCP- или UDP-пакет. **Алгоритм применения протокола ESP к исходящим IP-пакетам включает следующие шаги:**

1. Инкапсулируемый пакет копируется в буфер.

2. Далее к этому пакету в буфере приписываются дополняющие байты (поле Padding), их число (поле Pad Length) и тип первого заголовка инкапсулируемого пакета (поле Next Header); поле Padding выбирается та им, чтобы поле Next Header было прижато к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования.

3. Текущее содержимое буфера зашифровывается.

4. В начало буфера приписываются поля SPI и Sequence Number с соответствующими значениями.

5. Пополненное содержимое буфера обрабатывается по используемому алгоритму аутентификации, и после окончания этой процедуры в конец буфера помещается поле Authentication Data.

6. Формируется результирующий IP-пакет путем приписывания соответствующего IP-заголовка в начало буфера.

Структура IP-пакетов до и после применения протокола ESP показана на рисунке.

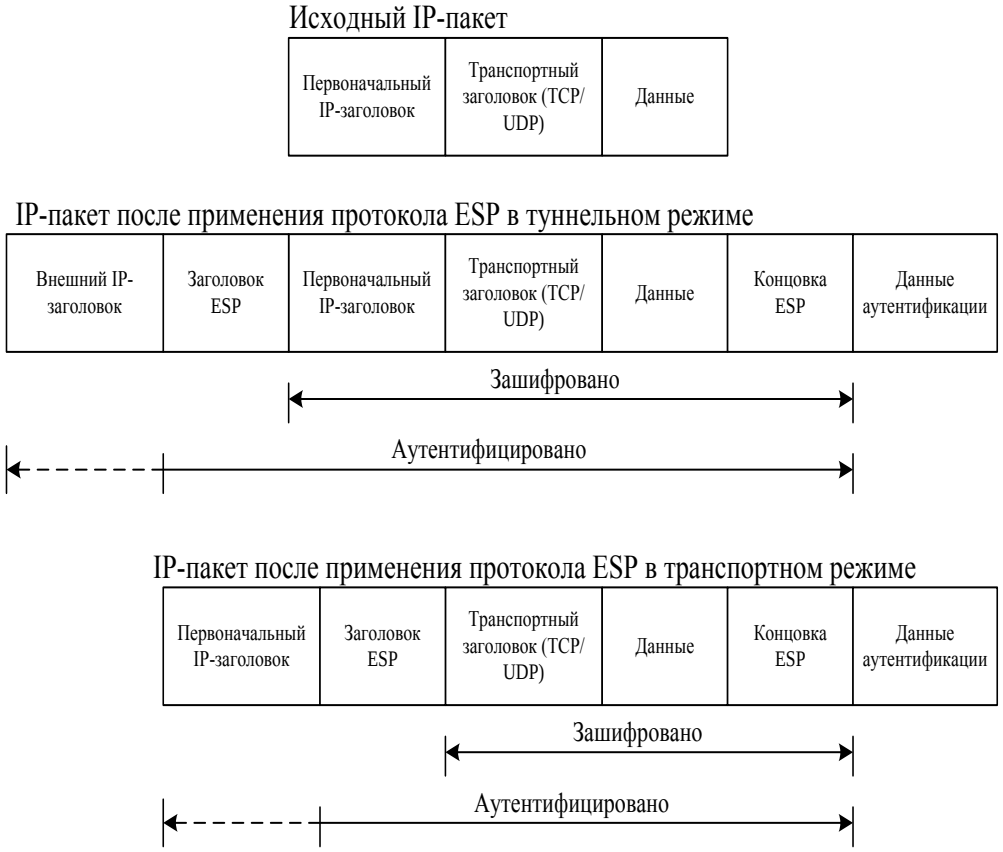


Рис. 9. Работа протокола ESP.

Таким образом, если в соответствии с протоколом ESP предусматриваются и криптографическое закрытие и аутентификация, то аутентифицируется зашифрованный пакет. Для входящих пакетов действия выполняются в обратном порядке, то есть сначала производится аутентификация. Это позволяет не тратить ресурсы на расшифровку поддельных пакетов, что в какой-то степени защищает от атак, ориентированных на отказ в обслуживании.

При использовании протокола ESP в туннельном режиме каждый исходный IP-пакет в криптозащищенном виде помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. Когда ESP используется в транспортном ре жиме, в конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета, и к полученному конверту добавляется исходный IP-заголовок.

Протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием, протокол AH должен приме пяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, в данном режиме допускается многократная вложенность туннелей с различными начальными и/или конечными точками. Поэтому в случае туннельного режима число возможных комбинаций по совместному использованию протоколов AH и ESP существенно больше.

Существуют две основные схемы применения протокола IPSek, отличающиеся ролью узлов, завершающих защищенный канал. В первой схеме защищенный канал устанавливается между оконечными УК сети Internet/ Intranet, а во второй – между шлюзами безопаснсости, которые устанавливаются на границе сети Internet. При этом оконечные УК сети Intranet не поддерживают IPSek, т. е. они передают трафик в корпоративной сети в незащищенном виде. Варианты относительного расположения заголовков пакетов в туннельном режеме «шлюз-шлюз» и режиме «хост-хост» совпадают.

В качестве методологической базы для анализа ТС инфокоммуникационной сети на технологии IP-QoS, удовлетворяющих перечисленным выше требованиям, будем использовать концепцию ее архитектуры. В рамках этой концепции, эффективность использования IP-сети с интеграцией служб в режиме установленного соединения по аналогии с [6] предлагается оценивать с помощью набора функционалов использования пропускной способности каждого ЛЦТ $ij \in J$, входящих в состав виртуального пути $\widehat{l}^{k}_{st,m} = \left\{ si_1, i_1 i_2, ..., i_{p-1} t \right\}^{k}_{st,m}$, трафиком различных классов и учитывающих особенности реализации протокола каждого логического уровня ТС.

Протокол ISAKMP описывает базовые процедуры аутентификации сторон, обмена ключами и согласования всех остальных параметров защищенного IPSec-туннеля. Однако он не содержит конкретные *алгоритмы обмена криптографическими ключами*. Поэтому для обмена ключами могут использоваться другие протоколы. В спецификации IPSec в качестве такого протокола, используемого при формировании общего защищенного туннеля, выбран *протокол Oakley*. Объединение протоколов ISAKMP и Oakley обозначают как ISAKMP/Oakley.

Эти протоколы представляют для нас интерес прежде всего как **средство разграничения прав доступа**. Действительно, ограничивать доступ к определенным сервисам инфокоммуникационной сети можно, основываясь **на системе распределения ключей.**

Принципы работы ISAKMP/Oakley, структура их заголовков и пакетов подробно рассмотрены выше. Отметим, что, несмотря на гибкие возможности этого протокола **по организации распределения прав доступа**, большой нагрузки на транспортную систему он (ISAKMP) не несет. При формировании контекста безопасности, помимо всего прочего согласуется и срок существования защищенного соединения, который зависит от требуемой криптостойкости. Согласно этому сроку определяется, как скоро, в зависимости от времени или объема переданных данных потребуется закрытие текущего соединения и возможно открытие нового. Этот параметр может быть задан не только для защищенного соединения, но и для защищенного канала.

Будем рассматривать ситуацию, когда срок существования защищенного соединения (в рамках канала) определен как 15 минут или 10 Мбайт, а срок существования самого канала – как 60 минут или 40 Мб. Понятно, что данные параметры зависят от длины используемых ключей, а также от криптостойкости применяемых алгоритмов. Такой подход позволяет сбалансировать криптографическую стойкость сервисов и стоимость накладных расходов на передачу ISAKMP-пакетов.

Схема создания защищенного канала выглядит следующим образом:

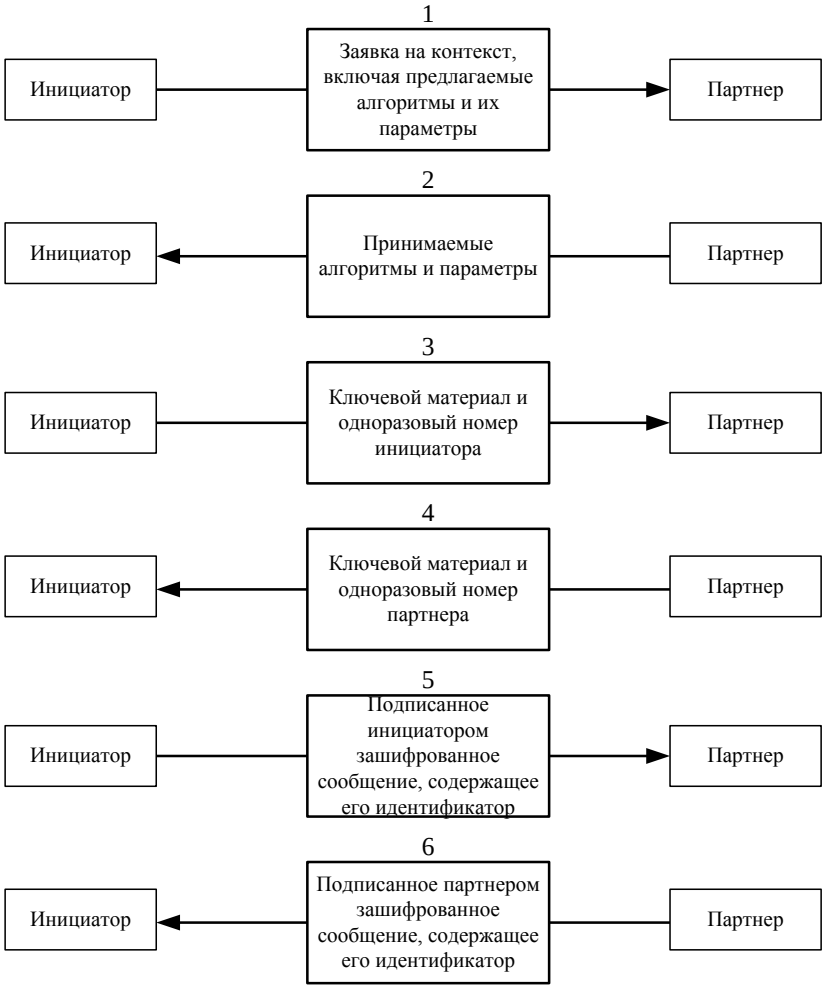


Рис. 23. Процедура создания защищенного канала.

Процедура формирования защищенного соединения существенно проще, так как глобальные параметры уже согласованы. Согласование параметров двух симметричных однонаправленных соединений осуществляется на основе формирования управляющего контекста с помощью трех шагов:

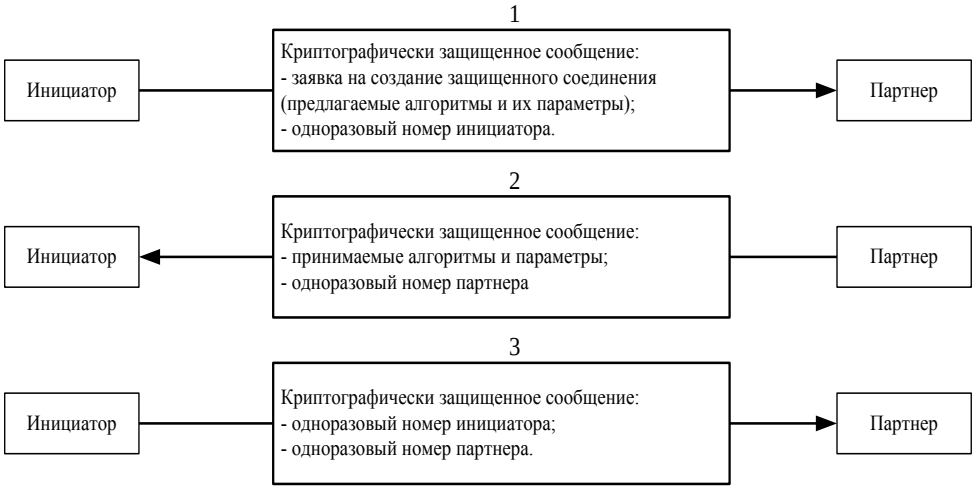


Рис. 24. Процедура создания защищенного соединения.

Будем считать, что один шаг данных схем предполагает послание 400 Кб служебной информации (из них – 28 байт – заголовок ISAKMP [8], 20 байт – заголовок IP). Таким образом, для создания защищенного туннеля необходимо передать 6*400 = **2400 байт служебной информации**. А для создания защищенного соединения в рамках данного туннеля – 3*400 = **1200 байт.**

Исходя из длительности существования **канала и соединения**, заданного в **мегабайтах (40 и 10 соответственно**), можно рассчитать, какой **процент служебной информации ISAKMP/Oakley уходит на передачу этих 40 (10) мегабайт.**

$$K_{канала} = \frac{2400}{41943040} = 0{,}000057$$

$$K_{соединения} = \frac{1200}{10485760} = 0{,}000114$$

Видим, что эти значения пренебрежимо малы, поэтому в дальнейших расчетах учитываться они не будут.

Как уже отмечалось, протокол IPSec обладает большой гибкостью, что позволяет использовать его возможности в различных вариациях. Каждый из вариантов вносит определенные изменения в структуру пакета на сетевом уровне, тем самым изменяя ВВХ системы. Ниже представлена схема, по которой будет происходить исследование и дальнейший анализ применения протокола IPSec как средства аутентификации и контроля доступа.

Рис. 13. Схема проведения исследования.

Исходные данные

Рассмотрим структуру IP-пакета. Он состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт (160 бит), имеет следующую структуру.

4 бита Номер Версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина
16 бит Идентификатор пакета		3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни	8 бит Протокол верхнего уровня		16 бит Контрольная сумма
32 бита IP-адрес источника			
32 бита IP-адрес назначения			
Параметры и выравнивание			

Рис. 14. Формат IP-заголовка.

Хотя в зависимости от дополнительной служебной информации, размер заголовка может достигать 60 байт, расчеты будем производить, исходя из его стандартной длины – **160 бит.**

Поле общая длина, занимающее 16 бит заголовка означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля и составляет 216=**65535 байт**, однако в большинстве случаев такие большие пакеты не используются. При передаче по сложной составной сети, длина пакета определяется с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Например, если это кадры **Ethernet,** то выбираются **пакеты с максимальной длиной 1500 байт**, умещающиеся в поле данных кадра Ethernet. Для сравнительных расчетов незащищенного режима работы сети и защищенного будет использоваться длина пакета 1500 байт (12000 бит).

Однако, чрезвычайно важно отметить, что при первом приближении, можно сказать, что большинство IP-пакетов, передающихся по сети имеют либо маленький размер (менее **128 байт**), либо большой (1500 байт). Маленькие пакеты используются **для передачи самой различной служебной протокольной информации**. Различные исследования показали, что гистограмма функции распределения длины пакета имеет следующий вид (данные взяты из работ Дуга Вайтинга (Doug Whiting), Брюса Шнаера (Brus Schneier), Стива Белловина (Steve Bellovin), AT&T Labs Research) [11]:

Рис. 15. Распределение вероятности появления пакетов.

Размер пакета (байт)	Распределение вероятности	Распределение пропускной способности
32	0	0
64	0,489	0,0602
96	0,055	0,0102
12	0,012	0,003

8		
160	0,006	0,0018
192	0,006	0,0022
224	0,006	0,0026
256	0,005	0,0025
288	0,016	0,0089
320	0,009	0,0055
352	0,008	0,0054
384	0,006	0,0044
416	0,005	0,004
448	0,004	0,0034
480	0,004	0,0037
512	0,003	0,003
544	0,01	0,0105
576	0,068	0,0754
1024	0,023	0,0453
1536	0,253	0,748

Исходя из приведенных данных можно сделать вывод, что большинство пакетов имеют небольшой размер, однако большинство байт, передающихся в канале находятся в больших пакетах. Чтобы не упустить из внимания данную особенность, вычислим математическое ожидание распределения случайной величины – размера IP-пакета, и его и будем использовать при расчетах. Для этого произведем несложный подсчет:

$$L_{ip}^{\ cp} = \sum_i L_{ip} \cdot P(L_{ip}) = 520(байт)$$

,

где P(Lip) – вероятность появления пакета длины Lip.

Скорость шифрования берется для расчета работы протокола AH при использовании алгоритма MD5. Это довольно быстрый алгоритм, в десятки и сотни раз (в зависимости от реализации) быстрее RSA. Есть данные, что на процессоре Pentium 90 Mhz его производительность составляет **108 бит/с**.

Lip	4160 (бит)	Длина IP-пакета
V	4*109 (бит/с)	Скорость передачи в ЛЦТ, содержащим данное виртуальное соединение
ω	64*103 (бит/с)	Скорость работы установки данных оконечной системы
Hip	160 (бит)	Длина заголовка IP-пакета
T	0,2 (с)	Среднее время пребывания пакета данных в n-звенном транспортном канале
N	4	Число переприемов в транспортном соединении
B	10-6	Вероятность ошибки в канале
Vш	1*108 (бит/с)	Скорость шифрования

В транспортном режиме в конверт IPSec помещается только содержимое защищаемого IP-пакета и к полученному конверту добавляется исходный IP-заголовок. Изменение структуры IP-пакета в данном случае имеет следующий вид [5]:

Рис. 16. Работа протокола AH в транспортном режиме.

Для дальнейших расчетов нам необходимо знать длину заголовка AH, который представлен на рисунке.

Next Header	Payload Len	Зарезервировано
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (переменная длина)		

Рис. 17. Формат заголовка AH.

Поля заголовка имеют следующие размеры [7]:
Next Header — 1 байт.
Payload Len — 1 байт.
Reserved (Зарезервировано) – 2 байта.
SPI — 4 байта.
Sequence Number — 4 байта.
Authentication Data — 16 байт (предполагаем, что используется алгоритм аутентификации MD5, дающий дайджест-функцию в размере 128 бит) [5].
Таким образом, имеем размер заголовка AH равным:
HIPSec = 224 бита.
В туннельном режиме защищаются все поля IP-заголовков. Каждый обычный IP-пакет помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля.

Рис. 17. Работа протокола AH в туннельном режиме.

По рисунку видно, что к исходному IP-пакету прибавился заголовок AH (224 бита при условии формирования дайджест-функции с помощью алгоритма MD5), а также новый IP-заголовок (160 бит). Итого
HIPSec = 384 бит
Транспортный режим ESP служит для шифрования и, если нужно, аутентификации данных, пересылаемых по протоколу IP (например, сегмента TCP). Для этого режима в случае с IPv4 заголовок ESP размещается в пакете IP непосредственно перед заголовком транспортного уровня (например, TCP, UDP,

ICMP), а концевик (trailer) пакета ESP (содержащий поля заполнителя, длины заполнителя и следующего заголовка) размещается после пакета IP; если же используется функция аутентификации, то поле данных аутентификации ESP добавляется после концевика ESP. Весь сегмент транспортного уровня вместе с концевиком ESP шифруются. Аутентификация охватывает весь шифрованный текст и заголовок ESP.

Алгоритм шифрования DES (Data Encryption Standard) с явно заданным вектором инициализации (Initialization Vector -- IV) применяют в протоколе ESP по умолчанию. Это блочный алгоритм шифрования с симметричным ключом. Его должны поддерживать все реализации IPSec, то есть он необходим для обеспечения IPSec-совместимости. В качестве альтернативы DES определены следующие алгоритмы: Triple DES, CAST-128, RC5, IDEA, Blowfish и ARCFour. По причине универсальности DES в реализациях IPSec он и будет рассматриваться при формировании поля Payload Data.

Базовым для протокола IPSec является режим ECB, для которого характерны разбиение открытого текста на 64-битовые блоки и их независимое шифрование при помощи одного и того же 64-битового ключа; Для шифрования используются 56 бит ключа из 64; оставшиеся 8 бит необходимы для контроля. Блок шифртекста, как и соответствующий ему блок открытого текста, имеет длину 64 бита.

В транспортном режиме работы ESP IP-пакет подвергается следующим преобразованиям:

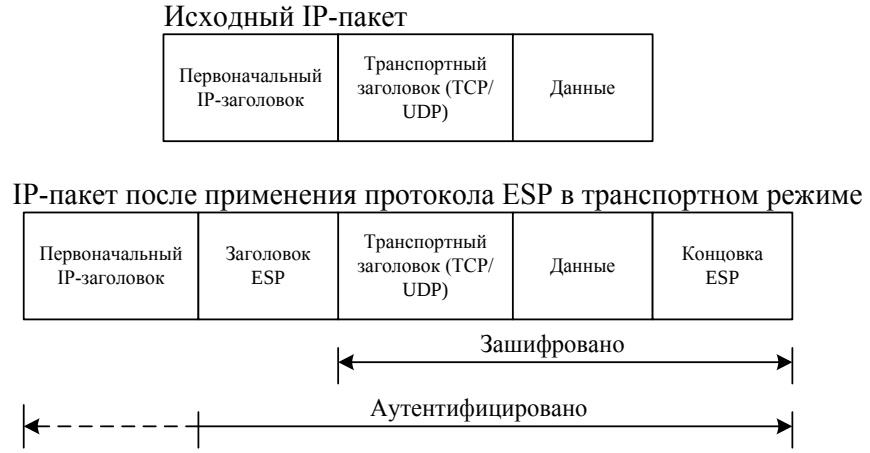


Рис. 18. Работа протокола ESP в транспортном режиме без AH.

Расшифровывая поля «Заголовок ESP» и «Концовка ESP» (ESP Trailer) можно изобразить данный IP-пакет следующим образом.

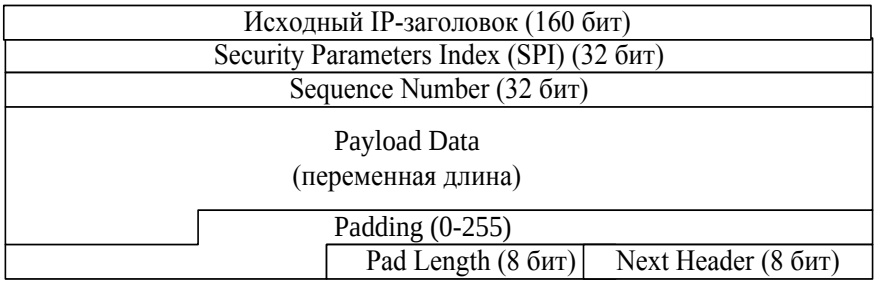


Рис. 19. Формат заголовка ESP (заголовок + trailer).

Таким образом, нам необходимо рассчитать длину шифруемой части и смещения (Padding). Как видно из рисунка, шифрованию подвергается информационная часть IP первоначального IP-пакета, без его заголовка (т.е. Lip-Hip=4000 бит) и Концовка ESP, которая состоит из двух полей по 8 бит и одного поля переменной длины. Алгоритм DES шифрует данные порциями по 64 бит, причем размер шифротекста равен размеру первоначальных данных (отмечалось ранее). Весь зашифрованный фрагмент должен нацело делиться на 64, так как если длина сообщения не кратна 64, оно дополняется справа недостающим количеством нулевых битов. Рассчитаем недостающие биты, входящие в поле Padding.

4000/64 = 62,5

Padding = 64*63 – 4000 = 32 (бит).

Таким образом «Концовка ESP» (ESP Trailer) имеет длину 32+8+8=48 бит.

Общая длина неинформационных битов, вносимых в IP-пакет при данном режиме работы равна:

HIPSec = 32+32+48 = 112 бит

Существуют различные аппаратные и программные реализации алгоритма DES. В качестве скорости шифрования возьмем значение 1*106 бит/с.

Vш = 106 бит/с.

При использовании аутентификации IP-пакет после преобразования IPSec выглядит следующим образом. В поле наших рассуждений необходимо отметить изменившееся значение HIPSec (служебной информации протокола) за счет прибавления к уже имеющимся 112 битам еще 128 бит дайджест-функции (по алгоритму MD5):

HIPSec = 240 бит.

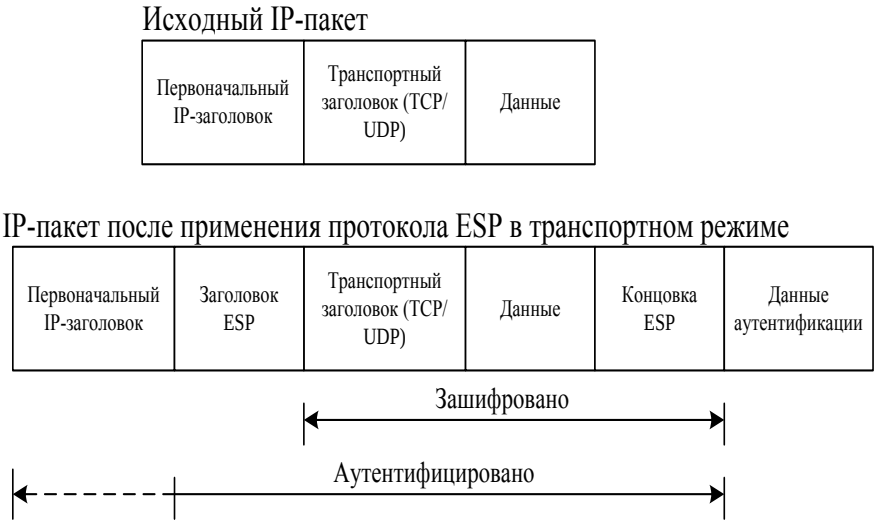


Рис. 20. Работа протокола ESP в транспортном режиме с АН.

При использовании протокола ESP в туннельном режиме каждый исходный IP-пакет в криптозащищенном виде помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет.

5.2.4.1 Применение протокола ESP в туннельном режиме без аутентификации АН

В данном случае преобразование IP-пакета происходит следующим образом:

Рис. 21. Работа протокола ESP в туннельном режиме без АН.

Относительно транспортного режима работы ESP и его служебной информации (HIPSec), в туннельном режиме к ней прибавляется длина внешнего IP-заголовка (160 бит). Таким образом, имеем:

HIPSec = 112 + 160 = 272 бит.

Применение протокола ESP в туннельном режиме с аутентификацией АН

В данном случае к преобразованный и зашифрованный пакет дополняется дайджест-функцией, аутентифицирующей отправителя. Ее длина – 128 бит (при использовании протокола MD5) прибавляется к

служебной информации IPSec:

HIPSec = 272 + 128 = 400 бит.

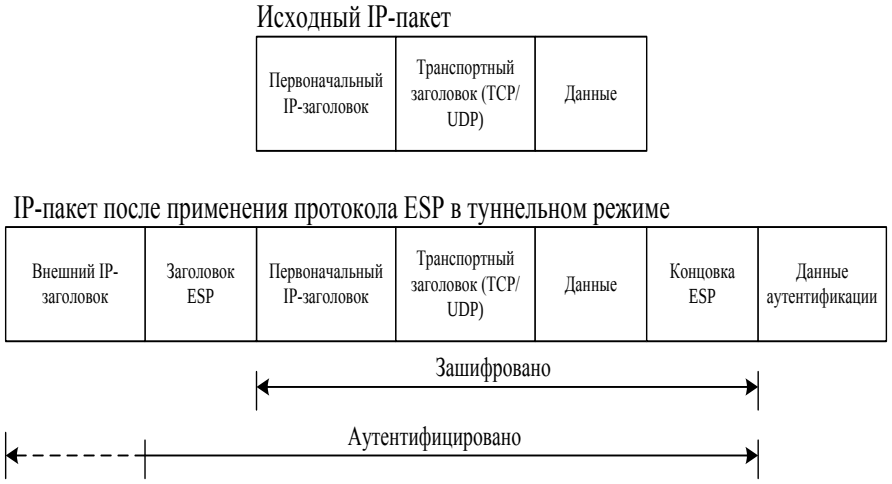


Рис. 22. Работа протокола ESP в туннельном режиме с AH.

Результатами же проведенных исследований являются значения эффективных скоростей передачи в ЛЦТ при использовании в качестве механизмов реализации аутентификации и контроля доступа протокола IPSec, средства которого позволяют на сетевом уровне осуществлять аутентификацию источника данных, их целостность, сокрытие, а также на основе систем распределения ключей по протоколам ISAKMP/Oakley организовывать разграничительную политику относительно прав доступа пользователей сети к ее сервисам.

О гибкости IPSec говорит различные режимы его работы, которые могут применяться в зависимости от поставленных задач, располагаемых ресурсов, и многих других факторов вплоть до законодательной базы страны применения. Так, например, туннельный режим обычно применяется для организации защищенного туннеля между специально выделенными защитными шлюзами (маршрутизаторы, защитные экраны). Его применение прозрачно для конечных пользователей. Транспортный же режим может применяться и для защиты конечных пользователей сети.

Базовую структуру IPSec можно представить тремя протоколами: AH (протокола, позволяющего аутентифицировать пакеты, а также некоторыми другими возможностями), ESP (протокола, обладающего всеми возможностями AH, но помимо этого способного к криптографическому сокрытию содержимого пакетов) и ISAKMP (протокола распределения ключей).

Исследование протокола ISAKMP, который описывает базовые процедуры аутентификации сторон, правила обмена ключами и согласование различных параметров защищенных соединений, показало, что какого бы то ни было существенного влияния на транспортную систему он не оказывает. Действительно, он вступает в действие лишь при создании защищенного канала, а также при создании в рамках этого канала одного или нескольких защищенных соединений.

Следует отметить, что среди параметров защищенных каналов и соединений есть и время их существования (в секундах или байтах переданной информации), незадолго до истечения которого происходит их переинициализация, следствием чего становится дополнительная служебная информация, переносимая по сети. Однако выяснилось, что даже с учетом этого, процент служебной информации ISAKMP/Oakley ничтожно мал по сравнению с информацией, вносимой протоколами AH или ESP в каждый пакет, передаваемый по сети.

Влияние протоколов AH и ESP рассматривалась при следующих режимах работы сети:

- применение протокола AH в транспортном режиме;
- применение протокола AH в туннельном режиме;
- применение ESP в транспортном режиме с аутентификацией AH;
- применение ESP в транспортном режиме без аутентификациеи AH;
- применение ESP в туннельном режиме без аутентификации AH;
- применение ESP в туннельном режиме с аутентификацией AH;

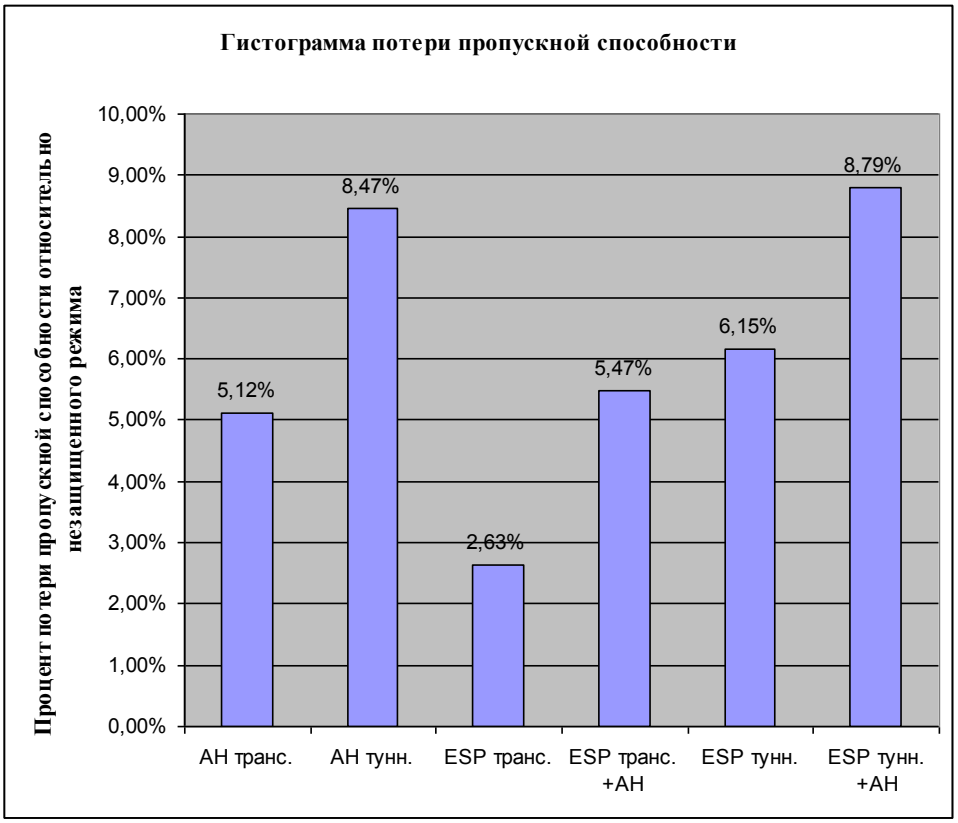
Кроме того, проводилось исследование влияния данных режимов при передаче IP-пакетов различной длины, а также при различной скорости передачи данных в линейно-цифровом тракте.

Так как основным фактором, определяющим влияние IPSec на эффективную скорость передачи, является размер IP-пакета и изменения, вносимые протоколами AH и ESP в его структуру, было важно выбрать для какого размера IP-пакета производить расчеты. Для этого были взяты за основу данные, полученные благодаря исследованиям специалистов компании AT&T [12], показывающие распределение вероятности появления пакетов различной длины в реальных сетях, а также показывающие на передачу пакетов какой длины больше затрачивается пропускная способность канала.

На их основе было вычислено математическое ожидание длины IP-пакета, передающегося по сети (в пределах от 32 до 1500 байт) и оно оказалось равным 520 байт.

Другим важным фактором, влияющим непосредственно на конечный результат являются алгоритмы хэширования и шифрования, применяемые в протоколах IPSec, ведь они имеют различные форматы и размеры выходной информации, ложащейся в основу преобразованного пакета. Так как IPSec это открытый стандарт, в его реализациях могут использоваться многие алгоритмы, но для обеспечения совместимости в любой реализации должны присутствовать алгоритм аутентификации сообщений MD-5, и алгоритм шифрования DES. Именно их применение и было взято за основу в данных исследованиях.

С учетом этого была получена гистограмма эффективных скоростей передачи в незащищенном режиме, а также в различных режимах работы IPSec, и гистограмма, показывающая потерю пропускной способности вследствие организации функций защиты информации (то есть относительно незащищенного режима).



Приведенные данные показывают, что в, зависимости от режима работы, примерно от 2 до 9 процентов пропускной способности канала уходит на реализацию механизмов защиты. С учетом применяемых алгоритмов, основную лепту в дополнительную нагрузку вносит протокол аутентификации АН, который к каждому пакету, независимо от его размера, помимо своего заголовка прибавляет дайджест-функцию размером 128 байт (для сравнения – стандартный IP-заголовок занимает 20 байт). Эта дайджест (хэш) функция и позволяет получателю однозначно аутентифицировать отправителя.

Lip	4160 (бит)	Длина IP-пакета
V	4*109 (бит/с)	Скорость передачи в ЛЦТ, содержащим данное виртуальное соединение
ω	64*103 (бит/с)	Скорость работы установки данных оконечной системы
Hip	160 (бит)	Длина заголовка IP-пакета
T	0,2 (с)	Среднее время пребывания ячейки данных в n-звенном транспортном канале
N	4	Число переприемов в транспортном соединении
B	10-6	Вероятность ошибки в канале
Vш	1*108 (бит/с)	Скорость шифрования

Скорость шифрования берется для расчета работы протокола АН при использовании алгоритма MD5. Это довольно быстрый алгоритм, в десятки и сотни раз (в зависимости от реализации) быстрее RSA. Есть данные, что на процессоре Pentium 90 Mhz его производительность составляет **108 бит/с.**

Протокол ESP с используемым алгоритмом шифрования DES сам по себе не вносит

значительной избыточности, если применяется в транспортном режиме, так как **по алгоритму DES информация шифруется блоками по 64 байта, и длина шифротекста на выходе равна длине исходного текста** [9]. Таким образом, в расчет берется **только заголовок ESP**, прибавляемый к пакету.

Самым же затратным с точки зрения потребления ресурсов (причем как транспортных, так и вычислительных) является режим использования протокола ESP в туннельном режиме с аутентификацией AH. В данном случае, служебная информация, присовокупляемая к исходному IP-пакету имеет длину 400 бит, и содержит в себе и данные аутентификации пакета, и заголовок/концовку ESP и внешний IP заголовок.

Исследование влияния размера исходных IP-пакетов на эффективную скорость передачи при использовании IPSec позволяет проследить, как резко снижается эффективность сети при большом количестве передаваемых в ней пакетов небольших размеров (менее 300 байт). Это позволяет сделать **вывод о нецелесообразности использования алгоритмов, например, аутентификации, в тех случаях, когда происходит обмен значительным числом небольших пакетов (как правило, служебной). Однако, как это зачастую бывает, это противоречит требованиям обеспечения безопасности, ведь именно при обмене служебной информацией наиболее важно обеспечить должный уровень безопасности.**

Практические исследования трафика

С целью проверить достоверность полученных результатов, были проведены практические исследования, на основе созданного защищенного IPSec-туннеля.

Для создания туннеля использовались встроенные средства **двух рабочих станций с предустановленной операционной системой MS Windows XP**, которые позволяют производить обмен данными в транспортном режиме с использованием следующих параметров безопасности [4]:

шифрование и обеспечение целостности (ESP+AH);

только обеспечение целостности (AH).

В рамках протокола **ESP** поддерживаются алгоритмы шифрования **DES и 3DES**, в рамках протокола **AH** – алгоритмы проверки целостности **MD5 и SHA1.**

Исследование проводилось на четырех этапах в зависимости от типа предоставляемого сервиса:

1. Файловый сервис. Передача файлов общим размером 580119 Кб.
2. Веб-сервис. Доступ к веб-серверу, расположенному на одной из машин.
3. Передача видео-сигнала (1 минута).
4. Потоковый звук (онлайн радио, 1 минута). При этом одна из машин использовалась в качестве шлюза доступа к сети Интернет.

6.1 Исходные данные

Тип туннеля	На основе предопределенного ключа
Значение ключа	daelgsardo
Скорость передачи в КС	100 Мбит/с
Конфигурации станций	**№1**: P4 2,66/512, Windows XP **№2**: Athlon XP 2500+/512, Windows XP
Средство измерения трафика	Программный комплекс Kerio Winroute Firewall 6.2.0
Размер передаваемых данных на первом этапе	580119 Кб
Алгоритм шифрования	DES
Алгоритм аутентификации данных	MD5

6.2 Ход исследования

В ходе исследования был измерен трафик, **переданный по сети**, а также время передачи с задействованными механизмами защиты и без оных. При этом менялись параметры туннеля: режим ESP+AH, режим AH.

Полученные данные сведены в таблицу:

Этап	Режим работы		
	Без IPSec	AH	ESP+AH
1. Передача файлов (580119 Кб)	Передано: 593942 Кб Время передачи: 1:55	Передано: 620474 Кб Время передачи: 2:10	Передано: 620598 Кб Время передачи: 2:13
2. Доступ к веб-серверу (одинаковые действия после очистки кэша)	Передано: 520,2 Кб	Передано: 538,2 Кб	Передано: 542,9 Кб
3. Передача видео-	Передано: 15236 Кб	Передано: 16080 Кб	Передано: 15893 Кб

сигнала (1 минута)			
4.Передача звукового сигнала (1 минута, качество 128 Кбит/с)	Передано: 1028 Кб	Передано: 1078 Кб	Передано: 1077 Кб

Процентные изменения количества передаваемой информации представлены в таблице расчетов:

Этап	Процентное увеличение передаваемой информации относительно незащищенного режима	
	AH	ESP+AH
№1	4,5% увеличение времени передачи – 13%	4,5% увеличение времени передачи – 15,6%
№2	3,5%	4,3%
№3	5,5%	4,3%
№4	4,9%	4,8%

Видим, что полученные экспериментальным путем данные соответствуют приведенным ранее расчетным (для AH и ESP+AH соответственно 5,12% и 5,47%). Можно заметить, что за исключением третьего этапа (передача видеосигнала в течение одной минуты) потери в режиме AH и ESP+AH приблизительно равны, что, с учетом конфигурации использовавшегося оборудования, говорит **о целесообразности использования шифрования информации наряду с обеспечением ее целостности.**

На третьем этапе уменьшение процентного соотношения обуславливается погрешностью измерений времени, так как за одну секунду передается порядка 254 Кбайт информации.

Различные же цифры на разных этапах отражают особенности передачи информации различного типа.

7. Общий вывод

Вопросам информационной безопасности (в том числе аутентификации и контроля доступа) в настоящее время уделяется значительно большее внимание, чем это было всего несколько лет назад, а в будущем, на пути все большей интеграции различного рода инфоуслуг в жизнь человека (в т.ч. и посредством инфокоммуникационных сетей), внимание вопросам безопасности будет только усиливаться.

Можно сказать, что применение механизмов аутентификации и контроля доступа в инфокоммуникационных сетях будущего будет в большой степени неотъемлемой их частью, и следовательно должны быть учтены затраты пропускной способности транспортной системы (да и сетей доступа) на реализацию этих механизмов.

Данная работа показывает, что при проектировании сетей следующего поколения, должны быть учтены затраты пропускной способности каналов связи (как транспортных, так и сетей доступа), которые по полученным данным составляют 5-9%. Расчетные данные были подтверждены экспериментальным исследованием защищенного IPSec-туннеля в типичной корпоративной сети. Можно отметить, что с учетом современных угроз информационной безопасности (как внешних, так и внутренних) применение исследованных механизмов обеспечения аутентичности и целостности данных вполне обосновано и в современных сетях различного типа, так как они обычно имеют необходимый резерв и по пропускной способности каналов и по производительности коммутационного оборудования.

Дальнейшие направления исследования

Можно наметить несколько путей дальнейших для исследований данной проблематики.

Во-первых, углубляясь в математические модели построения транспортных систем (на технологии IP или ATM) можно рассмотреть применение различных механизмов безопасности к различным типам трафика. Это позволит более гибко распределять имеющуюся пропускную способность каналов и вычислительную мощность узлов. Например, для изохронного трафика класса A можно применять алгоритмы аутентификации, а для асинхронного трафика класса D – не применять.

Далее, в рамках исследования протокола IPSec можно рассмотреть другие алгоритмы шифрования (например Triple DES, CAST-128, RC5, IDEA, Blowfish и ARCFour) и аутентификации (например SHA-1). Также в данной работе была не затронута возможность практически бесконечной вложенности туннелей, что может в значительной степени увеличить нагрузку на транспортную систему.

И, наконец, выходя за рамки протокола IPSec, можно исследовать другие протоколы и стандарты, способные реализовывать функции аутентификации и контроля доступа в сети (например, протокол Kerberos).

Литература

1. А.Т. Гургенидзе, В.И. Кореш «Мультисервисные сети и услуги широкополосного доступа», Наука и техника, Санкт-Петербург, 2003 г

2. А.Ю. Щеглов «Защита компьютерной информации от несанкционированного доступа», Наука и техника, Санкт-Петербург, 2004 г.

3. В. Зима, А. Молдовян, Н. Молдовян «Безопасность глобальных сетевых технологий», БХВ-Петербург, 2000 г.

4. Б. Сосински, Д. Московиц «Microsoft Windows 2000 Server», Вильямс, Москва, 2001 г.

5. Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

6. Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, August 1995.

7. Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

8. D. Maughan, M. Schertler, M. Schneider, J. Turner, “Internet Security Association and Key Management Protocol (ISAKMP)”, 1998.

9. C. Madson, N. Doraswamy, “The ESP DES-CBC Cipher Algorithm With Explicit IV”, RFC 2405, 1998.

10. В. Олифер, Н. Олифер, «Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд.», издательство «Питер», Санкт-Петербург, 2005 г.

11. D.Whiting, B.Schneier, S.Bellovin, “AES Key Agility in High-speed IPSec Implementations”, 2000.

12. Н.Н. Мошак, «Основы проектирования сетей АТМ. Методы и модели расчета параметров широкополосных цифровых сетей с интеграцией служб», СПб ГУТ им. проф. Бонч-Бруевича, Санкт-Петербург, 2003

(данные взяты из работ Дуга Вайтинга (Doug Whiting), Брюса Шнаера (Brus Schneier), Стива Белловина (Steve Bellovin), AT&T Labs Research) - Whiting, B.Schneier, S.Bellovin, “AES Key Agility in High-speed IPSec Implementations”, 2000 [11]

Вербальное описание асимметричных механизмов открытого шифрования

У. Диффи и М. Хелман в 1976 году [9] впервые показали, что секретность передачи информации может обеспечиваться без обмена секретными ключами в так называемых двухключевых или асимметричных криптосистемах. Криптосистемы с открытым ключом используют криптоалгоритм с двумя разными, но взаимосвязанными ключами. При этом открытый (общий) ключ доступен любому пользователю сети, а личный (секретный) ключ остается в личном пользовании. Ключи хотя и связаны между собой, но устроены так, что вычислить по открытому ключу второй личный практически невозможно. Преимущество двухключевых криптосистем обусловлено тем, что задача аутентификации открытых ключей намного проще и дешевле, чем задача распределения секретных ключей в одноключевых системах, которая для своего решения требует защищенных каналов. Использование асимметричных шифров можно свести к трем аспектам применения:

- *шифрование/дешифрование*, при котором отправитель шифрует сообщение M^k (или его сжатое отображение, являющееся функцией M^k) с использованием открытого ключа получателя;

- *цифровая подпись, когда отправитель «подписывает» сообщение M^k с помощью личного ключа;*

- *обмен ключами, при котором происходит обмен сеансовым ключом с применением личных ключей одной и/или обеих сторон.*

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций.

Открытый шифр Райвеста-Шамира-Адлемана (RSA). В качестве однонаправленной функции с секретом в криптосистеме RSA используется модульная экспонента с фиксированным модулем и показателем степени, т. е. схема блочного шифра RSA основана на выражениях со степенями. Переменное основание модульной экспоненты используется для представления числового значения сообщения M либо криптограммы C. Надежность криптоалгоритма RSA основывается на трудности факторизации больших чисел и вычисления дискретных логарифмов в конечном поле. В алгоритме RSA открытый y_i и личный x_i ключи, сообщение M и криптограмма C принадлежит множеству целых чисел $Z_p = \{0,1,2,..., p-1\}$, где p - модуль: $p = nq$. Здесь n и q случайные большие простые числа, которые выбираются равной длины и держатся в секрете. Множество Z_p с операциями сложения и умножения по модулю p образует арифметику по модулю p. Открытый ключ выбирается случайным образом так, чтобы выполнялись условия: $1 \lhd y_i \lhd \varphi(p)$; $НОД(y_i, \varphi(p))=1$, где $\varphi(p)=(n-1)(q-1)$ функция Эйлера, которая указывает количество положительных целых чисел в интервале от 1 до p, взаимно простых с p. Второе условие означает, что ключ y_i и функция $\varphi(p)$ должны быть взаимно простыми. Далее, используя расширенный алгоритм Евклида, вычисляется личный ключ x_i, при котором $x_i\, y_i \equiv 1(\mathrm{mod}\,\phi(p))$ или $x_i = y_i^{-1}(\mathrm{mod}(n-1)(q-1)$. Числа x_i и p должны быть взаимно простыми. Процедура шифрования на стороне отправителя s: $C = E_{y_t}(M) = M^{y_t}(\mathrm{mod}\, p)$. В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю p. Получатель t расшифровывает сообщение C на своем личном ключе x_t: $M = D_{x_t}(C) = C^{x_t}(\mathrm{mod}\, p) = (M^{y_t})^{x_t} = (M)^{y_t x_t}(\mathrm{mod}\, p)$.

Схема асимметричного шифрования RSA состоит в следующем: каждый отправитель s и получатель t сети генерируют по паре ключей каждый – открытый (y_s, y_t) для шифрования и секретный (x_s, x_t) для расшифрования; открытые ключи вида (y_s, p) опубликовываются в доступном для всех реестре или файле. Отправитель s разбивает сообщение M на блоки: $M = \{M_i\}, i = \overline{0, p-1}$ и шифрует последовательность чисел M_i по формуле $C_i = (M_i)^{y_t}(\mathrm{mod}\, p)$. Получатель t расшифровывает принятую последовательность криптограмм $M_i = (C_i)^{x_t}(\mathrm{mod}\, p)$ и восстанавливает сообщение M.

RSA Data Security утверждает, что при использовании функции маскирования общая ***производительность снижается на величину от 2 до 10%*** [10].

Кроме алгоритма RSA к асимметричным алгоритмам относятся алгоритм открытого распределения ключей Диффи-Хелмана , алгоритм ассиметричного шифрования Эль-Гамаля, асимметричная криптосистема ECC на эллиптических кривых и др. Уникальность алгоритма ***Диффи-Хелмана*** заключается в том, что пара корреспондентов в сети имеет возможность получить известный только им разделяемый секрет, передавая по открытой сети открытые ключи. Сообщения шифруются с использованием полученного общего секрета с применением симметричного шифрования. Однако указанный алгоритм используется, в основном, для распределения ключей.

Вероятностный открытый шифр Эль-Гамаля. Алгоритм шифрования Эль-Гамаля использует дополнительно разовый сеансовый открытый ключ и заключается в следующем [9]. Отправитель s выбирает случайное число K_{x_s} (разовый секрет); вычисляет открытый ключ $K_{y_s} = \alpha^{K_{x_s}} (\mathrm{mod}\, p)$; используя открытый ключ K_{y_t} вычисляет ***разовый общий секрет*** $K_{st} = K_{y_t} \alpha^{K_{x_s}} (\mathrm{mod}\, p)$; зашифровывает сообщение M с помощью умножения по модулю p сообщения M на разовый общий секретный ключ: $K_{st}\, M \ (\mathrm{mod}\, p) = C$; отправляет получателю t шифрограмму (K_{y_s}, C). Алгоритм расшифрования: $M = C\ /(K_{y_s})^{x_t} = C\ / K_{st} (\mathrm{mod}\, p)$.

Таким образом, суть открытого шифрования Эль-Гамаля состоит в использовании умножения по модулю сообщения на разовый общий секрет. Безопасность алгоритма асимметричного шифрования Эль-Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле. Для того чтобы получатель t мог правильно расшифровать сообщение, в криптограмму вместе с шифрограммой C^k включается также и разовый открытый ключ y_s отправителя, что приводит к увеличению размера криптограммы примерно в 2 раза по сравнению с исходным сообщением. Алгоритм Эль-Гамаля может использоваться как для шифрования, так и для ЭЦП.

На практике в сетях общего пользования применяются гибридные криптосистемы, в которых сообщение шифруется с помощью одноключевых шифров, а распределение сеансовых симметричных секретных ключей осуществляется по открытому каналу с помощью двухключевых шифров. В этом случае общий сеансовый секрет используется для шифрования симметричных ключей, а последние, - для шифрования сообщений. Это связано с тем, что в двухключевых криптосистемах шифрование/дешифрование предполагает использование операции возведения в степень по модулю 500-1000-битовых

чисел, что при программной реализации в десятки раз медленнее, чем шифрование того же сообщения симметричным алгоритмом [9].

2.2.1.4. Модели процессов задействования асимметричных механизмов шифрования

Механизмы шифрования задействуются в начале сессии после завершения транзакции контроля допустимости установления соединения. Применение асимметричных механизмов шифрования порождает потоки служебных сообщений при распределении открытых ключей $\rho_{y_t}^{распр}$ (***пять служебных сообщений для обмена пользователей сети с центром CA с периодичностью времени действия сертификата***) и их аутентификации $\rho_{y_t}^{аут}$ (***два сообщения аутентификации на каждое вызывное сообщение***), а также аутентификации корреспондентов при создании общего сеансового секрета $\rho_{K_{st}}^{аут}$ (***двух- или трехразовое «рукопожатие»***). Интенсивность указанных потоков зависит от интенсивности поступления $\lambda_{выз}^{k}$ вызывных сообщений. Любая транзакция шифрования состоит из двух фаз: а) фазы **создания общего сеансового секрета** K_{st} и б) фазы шифрования/расшифрования сообщения с помощью симметричного алгоритма. Фаза **создания ключа** K_{st} включает в себя время, затрачиваемое на распределение $t_{y_i}^{распр}$ и аутентификацию $t_{y_i}^{аут}$ открытых ключей корреспондентов y_i, получаемых по запросу из центра сертификации CA, и собственно время формирование секрета $t_{K_{st}}$. Управляющий трафик безопасности учитывается в моделях ТС с более низким относительным приоритетом обслуживания по отношению к базовым трафикам классов B и/или C в сессии. Здесь мы имеем дело с многофазной СМОУб. Процесс создания общего ключа K_{st} с учетом аутентификации источника можно формализовать в виде следующей аддитивной формулы

$$t_{st}^{k} = t_{y_i}^{распр} + t_{y_t}^{аут} + t_{K_{st}} + t_{K_{st}}^{аут}.$$

Здесь $t_{K_{st}}^{аут}$ - время на проведение процесса аутентификации («рукопожатия») или процедуры, которая позволяет удостовериться получателю/отправителю, что секретный ключ принадлежит законному отправителю/получателю. Общее время, затрачиваемое на шифрование сообщения в асимметричной системе, включает в себя время формирование общего секрета K_{st} с учетом установления подлинности источника и время симметричного шифрования на ключе, который вычисляется как сумма или произведение этих ключей.

Таблица 2.5.

Тип шифра	**Формализация процесса открытого шифрования**	**Временная избыточность**	**Протокольная избыточность**	**Потоковая избыточность**
Шифр RSA	$t^k_{убш\_асим} = t^{распр}_{y_i} + t^{аут}_{y_t} + t_{K_{st}} + t^{аут}_{K_{st}} + t^k_{убш}$	$t^k_{убш} + t_{st}$	нет	$\rho^{распр}_{y_t}$, $\rho^{аут}_{y_t}$, $\rho^{аут}_{K_{st}}$

Таким образом, процесс открытого шифрования в общем виде можно формализовать следующей аддитивной формулой

$$t^k_{убш\_асим} = t_{st} + t^k_{убш}.$$

Формализация процессов асимметричного шифрования и виды вносимой избыточности в процессы обработки и передачи основных информационных потоков в системе на примере шифра **RSA** приведены в табл.2.5.Пусть $a^{выз}_{st}(k)$ нагрузка вызывных сообщений, инициируемая узлом s в направлении узла t (пакет/с). Параметры трафика аутентификации для основных служб МСС приведены в таб. 2.6.

Таблица 2.6. Параметры трафика аутентификации для основных служб МСС

Тип трафика	**Число вызовов в ЧНН,** $\lambda^{выз}_{аб}$ **(сооб/час)**	**Нагрузка в ЧНН,** ρ^k **(эрл)**	**Длительность сессии,** τ^k_{ses}**,(с)**	$\lambda^{аут}$ **(сооб/час)**	$\rho^{аут}$ **(эрл)**
Телефония					
Квартирный сектор	3,6	0,1	100		
Деловой сектор	14,4	0,4	100		
Мини-АТС	21,6	0,6	100		
IP-телефония	14,4	0,4	100		
Видео					
Неподвижное изображение	12,0	0,2	60		
Телефакс	0,6	0,01	60		
Факс цветной	0,6	0,02	120		
Видеотелефон H.262	0,72	0,02	100		
Видеоконференции	0,6	0,1	600		
ТВВЧ	0,5	0,5	3600		
MPEG-1	1,5	0,5	1200		
MPEG-2/TV	1,0	0,5	1800		
MPEG-2/VCR	2,0	0,5	900		
Данные					

Интерактивный обмен данными	36,0	0,3	30
Передача файлов	18,0	0,05	10
Передача больших массивов данных	0,3	0,01	120
Поиск документов	3,0	0,25	300

Удельная нагрузка $\lambda^{aym}_{ij_{st,m}}(k)$, создаваемая в канале $ij \in l^k_{st,m}$ управляющим трафиком аутентификации при а) двух- и б) трехразовом «рукопожатии» при установлении подлинности отправителя соответственно будет равна

$$\lambda^{aym}_{ij_{st,m}}(k)=\begin{cases}(2\div 3)\lambda^{выз}_{st,m}(k)N/3600, ij \in l^k_{st,m}\\ O, ij \notin l^k_{st,m}\end{cases}.$$

$\lambda^{выз}_{st,m}(k)N\ t_{зан}=a^{выз}_{st,m}(k)=a^{выз}_{st}(k)p^{выз}_{st,m}(k)$(эрл), - трафик вызывных сообщений в m -ом пути тракта. $st \in S^k$. Общая нагрузка вызывных сообщений, поступающая в сеть $a^{выз}(k)=\sum_{st\in S^k} a^{выз}_{st}(k)$ в общем случае задана в виде матриц $Y^{выз}(k)=\left\|a^{выз}_{st}(k)\right\|$. Если V_{ij} - пропускная способность (бит/с) ЛЦТ $ij \in J_{st}$,, $\mu^k_{ij}=\frac{V_{ij}}{L^k}$ - интенсивность обслуживания в нем пакета; L^k - длина пакета аутентификации (бит), то загрузка $\rho^{aym}_{ij}(k)$ канала $ij \in J_{st}$, определяется по формуле

$$\rho^{aym}_{ij}(k)=\sum_{st\in S^k}\sum_{m=1}^{M^k_{st}}\frac{\lambda^{aym}_{ij,st,m}(k)}{\mu^k_{ij}}.$$

Если рассматривать МСС с R^k относительными приоритетами $r^k=\overline{1,R^k}$ в k-ом классе трафика, то загрузка ρ^k_{ij} канала $ij \in J_{st}$ определяется как $\rho^k_{ij}=\sum_{r^k=1}^{R^k}\rho^k_{ij,r^k}$, где ρ^k_{ij,r^k} - загрузка канала $ij \in J_{st}$ пакетами r^k - го приоритета. Эту величину будем вычислять по формуле $\rho^k_{ij,r^k}=\sum_{st\in S^k}\sum_{m=1}^{M^k_{st}}\frac{\lambda^k_{ij,st,m}(r^k)}{\mu^k_{ij}}$, где $\lambda^k_{ij_{st,m}}(r^k)\ N\ t_{выз}=a^k_{st}(r^k)$ - трафик r^k - го приоритета в тракте $st \in S^k$.

Можно рассмотреть два варианта обслуживания трафика аутентификации: 1) с относительным приоритетом более низкого порядка по сравнению с обслуживанием основного трафика в сессии или 2) с одинаковым приоритетом обслуживания основного трафика в порядке поступления. В первом случае общее время пребывания заявок в СМО типа $M/M/1$ ***дается выражениями***

$$T^k_{ij}=\frac{1}{1-\rho^k}\frac{\mu^{aym}+\mu^k\rho^{aym}}{\mu^k\mu^{aym}}$$

$$T_{ij}^{aym} = \frac{1}{\mu^{aym}} \frac{\rho^k/\mu^k + \rho^{aym}/\mu^{aym}}{(1-\rho^k)(1-\rho^k-\rho^{aym})}.$$

Мы будем рассматривать второй вариант. Для второго варианта время ожидания в очереди будет обусловлено интерференцией со всем поступающим трафиком и состоит частично из времени, зависящего от трафика данных (речи), и частично из времени, зависящего от трафика аутентификации. Обозначим $1/\mu^k$ ***среднюю длительность обслуживания пакета трафика класса*** k**, а через** $1/\mu^{aym}$ **- среднюю длину обслуживания всех пакетов (с учетом трафика аутентификации). Тогда выражение для** T_{ij}^k **будет иметь вид**

$$T_{ij}^k = \frac{\lambda_{ij}/\mu^*}{\mu^* - \lambda_{ij}} + \frac{1}{\mu^k}, \quad \textit{где} \quad \lambda_{ij} = (\lambda_{st,m}^{выз}(k) + \lambda_{ij_{st,m}}^{aym}(k))/3600 \textit{ (1/с)}, \quad \mu^* = \frac{\mu^k + \mu^{aym}}{2} \textit{ (1/с)},$$

$$\mu^k = \frac{V}{L^k + H_{IN}}, \ \mu^{aym} = \frac{V}{L^{aym} + H_{IN}},$$

Исходные данные: $L^{aym} = 350$ ***(бит) – вариант №1;*** $L^{aym} = 1500$ ***(бит) – вариант №2.***

$\lambda_{st,m}^{выз}(B) =$ ***3,6/час,*** $t_{зан}^B =$ ***100с;*** $\lambda_{st,m}^{выз}(C) =$ ***36/час,*** $t_{зан}^C =$ ***30с;*** $\lambda_{ij_{st,m}}^{aym} =$ ***1)2*** $\lambda_{st,m}^{выз}(k)$***;3*** $\lambda_{st,m}^{выз}(k)$***;***

$$t_{зан}^{aym} = \frac{L^{aym} + H_{IN}}{V}.$$

(Кирпич2)Текущая загрузка ЛЦТ базовыми потоками ρ_{ij}^B и ρ_{ij}^C в МСС на технологии IP-QoS с учетом абсолютного приоритета обслуживания речевых пакетов (с дообслуживанием) по отношению к пакетам данных дается соответственно выражениями [86] (3.9) и (3.12). Служебные пакеты трафика аутентификации, могут обрабатываться на маршрутизаторах с более низким или равным приоритетом по отношению к пакетам основных потоковых компонент. В предположении, что они обслуживаются в сети с одинаковым приоритетом для пакетов данных, то коэффициент загрузки ЛЦТ l-ой потоковой компонентой трафика безопасности (например, аутентификации, восстановления целостности, заполнения трафика). в общем виде можно представить как

$$\rho_{ij}^{*l} = \frac{L^* + H_{NA}}{L^* - H_{IP}} \frac{Mark_{ij}^C \Theta^{\min}}{V_{ij}} a_{ij}^{*l}, \qquad (3.86)$$

Для фазы установления мультимедийного соединения

$$a_{ij}^{*l} = a_{ij}^{*ycm} = N_{ij}^{multy} Mark_{ij}^{multy} \lambda_{ij}^{multy} (1 - b^{malty}) \theta_{ij}^* Mn^*. \qquad (3.87)$$

Здесь θ_{ij}^* - непроизводительное время занятия ЛЦТ трафиком безопасности на фазе установления мультимедийного соединения, час; L^* - длина служебного пакета трафика безопасности, бит; Mn^* - математическое ожидание числа служебных пакетов трафика

безопасности, приходящихся на один мультимедийный вызов, при формализации процессов аутентификации равноправных логических объектов.
Для фазы сессии

$$a_{ij}^{*l} = a_{ij}^{*ses} = N_{ij}^{multy} Mark_{ij}^{C} \ \lambda_{ij}^{C} \ \theta_{ij}^{ses*} \ Mn^{*}, \qquad (3.88)$$

где λ_{ij}^{C} - интенсивность поступления в ЛЦТ пакетов данных, пакет/час; θ_{ij}^{ses*} - непроизводительное время занятия ЛЦТ трафиком безопасности в сессии, час.

При сделанных выше предположениях суммарный коэффициент загрузки ЛЦТ трафиком данных и трафиком безопасности будет иметь следующий вид

$$\rho_{ij}^{*Cp} = \rho^{*Cp}(L^{*C}, T_{ij}^{*C}) + \sum_{l} \rho_{ij}^{*l} = (1 - \rho_{ij}^{Bp} - \frac{L^{*Cp} + H_{NI}}{T_{ij}^{*Cp} V_{ij}} - \frac{\rho_{ij}^{*Bp}}{1 - \rho_{ij}^{*Bp}} \frac{L^{*Bp} + H_{NI}}{T_{ij}^{*Cp} V_{ij}}) + \sum_{l} \rho_{ij}^{*l}, \qquad (3.89)$$

где, ρ_{ij}^{*l} - величина коэффициента загрузки l-ой потоковой компоненты трафика безопасности (например, аутентификации, восстановления целостности, заполнения трафика).

Коэффициент загрузки ЛЦТ речевым трафиком с учетом трафика безопасности $\hat{a}_{ij}^{*Bp} = \hat{a}_{ij}^{Bp} + a_{ij}^{*ses}$

$$\rho_{ij}^{*Bp} = \frac{L^{*Bp} + H_{NA}}{L^{*Bp} - H_{IP}} \frac{\upsilon^{Bp}}{V_{ij}} \ \hat{a}_{ij}^{*Bp} \ z^{Bp} \ \eta^{Bp}. \qquad (3.90)$$

Таким образом, минимально возможная эффективная скорость $V_{st}^{A_g \min}$ передачи трафика класса A в однородном тракте гибридной ИТС –определяется выражением (3.68), а минимально возможная эффективная скорость $V_{st}^{C_g \min}$ передачи трафика класса C в однородном тракте гибридной ИТС – выражением (3.69) при значениях оптимальных длин протокольных блоков l_{optCIF}^{A} и $l_{optCIF}^{C_g}$, рассчитанных по формулам (4.32) и (4.33)
или (4.34).

Предположим, что задачи (4.21) и (4.23) для однородной пакетной ИТС на технологии АТМ решены и допустимые значения разнородного трафика в сети $\rho_{ij}^{B_g^p \max}$, $\rho_{ij}^{C_g^p \max}$ найдены. Для того чтобы для нагрузки класса B, заданных матрицей Y^B и распределением потоков, выполнялись требования по передаче, необходимо выполнение системы неравенств: $\hat{\rho}_{ij}^{B_g^p} \le \rho_{ij}^{B_g^p \max}$, $\forall ij \in J$, где величины $\rho_{ij}^{B_g^p \max}$ рассчитываются по формуле (3.42) при решении задачи анализа. Таким образом, основное условие пропускания нагрузки класса B на примере сжатого цифрового речевого сигнала в сети АТМ-CIF определяется выражением $\eta^B z^{B_g^B} \frac{l_{opyCIF}^{B_g^P} + H_{ATM}}{l_{optCIF}^{B_g^P} - H_{SAR}^{B}} \frac{\upsilon^B \hat{a}_{ij}^{B_g^p}}{V_{ij}} \le \rho_{ij}^{B_g^p \max}$. Если на каком-либо звене $ij \in J_{st}$ условие не выполняется, то для всех $a_{ij}^{B_g^p} \ne 0$: $ij \in R_{st}^{B_g^p}$ требуемая речевая нагрузка в составе мультимедийных соединений не может быть пропущена через сеть с заданными «потерями» d^B. Типичные значения удельной нагрузки, создаваемой оконечными устройствами различных классов, и число вызовов в ЧНН для ИКС приведены в [45]. Ясно, что для трафика класса C должно выполняться неравенство (при $p = 0$)

$$\Theta^{\min} a_{st}^{C_g^p} \le V \frac{l_{optCIF}^{C_g^p} - H_{SAR}^{ABR}}{l_{optCIF}^{C_g^p} + H_{ATM}} (1 - \rho_{st}^{B_g^p} - \left[\frac{l_{optCIF}^{C_g^p} + H_{ATM}}{T_{st,m}^{C_g^p} - T_{pac}^{C}} \right] \frac{n}{(1 - \rho_{st}^{B_g^p})V}), \quad (4.35)$$

где $a_{st}^{C_g^p}$ – общая нагрузка ячеек данных класса C, поступающая в тракт $st \in S^{C_g^p}$ в рамках организации мультимедийных соединений. В общем случае, если обозначить через $\hat{a}_{ij}^{C_g^p}$ нагрузку ячеек данных класса C на звене, равную $\hat{a}_{ij}^{C_g^p} = \sum_{st \in S^{C_g^p}} \sum_{m=1}^{M_{st}^{C_g^p}} p_{st,m}^{C_g^p} \hat{a}_{st,m}^{C_g^p}$ для всех $st \in S^{C_g^p} : ij \in l_{st,m}^{C_g^p}$, то для трафика данных класса C должно выполняться условие

$$\Theta^{\min} \hat{a}_{ij}^{C_g^p} \le V_{ij}^{\min C_g^p}, \forall ij \in J_{st}. \quad (4.36)$$

Основное условие пропускания речевой нагрузки в гибридной ИТС при решении задач (4.25) и (4.27) с учетом $b_{ij}^{A} \le b^{A}$ принимает следующий вид

$$V_{ij}^{A} \le \upsilon^{A} \hat{a}_{ij}^{A_g}. \quad (4.37)$$

Если это не выполняется на каком-либо звене сети, то $\forall \; ij \in R_{st}^{A} : a_{st}^{A} \ne 0$, указанный речевой трафик класса A обслужен быть не может с заданными нормами b_{ij}^{A}. Если обозначить $\hat{a}_{ij}^{C_g}$ величину текущего трафика пакетов данных класса C в канале $ij \in R_{st}^{C_g}$, равную $\hat{a}_{ij}^{C_g} = \sum_{st \in S^{C_g}} \sum_{m=1}^{M_{st}^{Cg}} p_{st,m}^{C_g} \hat{a}_{st,m}^{C_g}, \quad \forall st \in S^{C_g} : ij \in l_{st,m}^{C_g}$, то условием его обслуживания с учетом $b_{ij}^{Cg} \le b^{Cg}$, потоков других направлений и заданных ограничений на качество передачи будет (при $p = 0$)

$$\Theta^{\min} \hat{a}_{ij}^{C_g} \le V^{Э} \frac{l_{optCIF}^{Cg} - H_{SAR}^{ABR}}{l_{optCIF}^{Cg} + H_{ATM}} (1 - n \frac{L + H_{ATM}}{(T_{st}^{C_g} - \frac{L - H_{SAR}^{ABR}}{\omega^{C}})V^{Э}}) \; \forall ij \in J^{C_g}. \quad (4.38)$$

Если это условие не выполняется на каком-либо канале $ij \in R_{st}^{C_g}$, то $\forall a_{st}^{C_g} : a_{st}^{C_g} \ne 0$, заданная нагрузка данных не может быть передана с требуемым средним временем $T_{ij}^{C_g}$ через гибридную ИТС на технологии ATM-SIF.

Предлагаемый выше метод расчета основных числовых характеристик транспортного соединения гибридной ИТС базируется на подсчете среднего числа линий, занятых речевой нагрузкой класса A. Для построения более точных методик, учитывающих динамику процесса перемещения физической или логической границы между трафиками обоих классов, можно построить модель n-звенного тракта передачи в гибридной ИТС, базирующуюся на методе квазистационарного состояния или методе текущей аппроксимации, как это сделано в работе [242] для однозвенного тракта.

Протоколы аутентификации можно классифицировать в соответствии со следующими параметрами [14-15]: тип аутентификации, тип используемой криптосистемы, вид реализации криптосистемы, количеству обменов служебными сообщениями между субъектами. Дополнительно они могут различаться наличием диалога и доверия между субъектами, а также использованием в протоколах отметок времени. Известно [5], что предоставление механизмов защиты осуществляется по принципам предоставления сервиса базовой эталонной модели взаимодействия открытых систем.

Не теряя общности формализуем процесс аутентификации равноправных логических объектов на примере простой аутентификации *без защиты с центром сертификации* (Authentication Center, CA). Процесс аутентификации с центром *CA* предполагает установления дополнительных ассоциаций, описываемых многофазными и/или однофазными СеМО, и порождает дополнительный служебный трафик безопасности, обслуживаемый в сети, с относительным или абсолютным приоритетом по отношению к базовому типу трафика данных класса *C* [11]. В этом случае транзакция аутентификации включает в себя следующие фазы: 1) отправитель i передает получателю в открытом (незащищенном) виде свой идентификатор (имя) ID_i и (необязательно) пароль Pi за время $t_{ij}^{прдIDi,Pi}$; 2) получатель j передает ID_i и Pi за время $t_{jCA}^{прдIDi,Pi}$ центру CA для сопоставления за время $t_{CA}^{обрPi}$ с Pi, который хранится у него в качестве атрибута; 3) центр CA подтверждает или отрицает получателю j действительность удостоверений за время $t_{CAj}^{прдPi}$; 4) успешность или неуспешность аутентификации может быть сообщена отправителю i за время $t_{ji}^{прдPi}$.

Процесс простой аутентификации равноправных логических объектов с центром *CA* на фазе установления мультимедийного соединения можно формализовать аддитивной формой вида [11]

$$t_{без}^{аут} = t_{ij}^{прдIDi,Pi} + t_{jCA}^{прдIDi,Pi} + t_{CA}^{обрPi} + t_{CAj}^{прдPi} + t_{ji}^{прдPi} \qquad (9)$$

При этом потоковая избыточность, порождаемая трафиком аутентификации в соответствии с вербальным описанием этого процесса формализуются аддитивной формой

$$\rho_{без}^{аут} = \rho_{ij}^{аут} + \rho_{jCA}^{аут} + \rho_{CAj}^{аут} + \rho_{ji}^{аут}. \qquad (10)$$

Здесь $\rho_{ij}^{аут}$; $\rho_{jCA}^{аут}$; $\rho_{CAj}^{аут}$; $\rho_{ji}^{аут}$ - соответственно коэффициенты загрузки составного тракта при передаче пароля P_i отправителя i к получателю j; от получателя j к центру *CA*; от центра *CA* к получателю j; от получателя j к отправителю в сигнальном пакете длины L^{RSVP} (бит).

В предположении, что время сопоставления пароля на центре *CA* $t_{CA}^{обрPi}$ незначительно в сравнении с временем его передачи по сети выражение для среднего времени транзакции аутентификации (с учетом, что $t_{ij}^{аут} = \dfrac{1}{\mu_{ij}^{аут}(1-\rho_{ij}^{аут})}$ - среднее *время пребывания сигнального пакета в канале* ij *имеет экспоненциальное распределение со средним* $1/\mu_{ij}^{аут}$ *и* независимости задержек в каналах трактов передачи) можно формализовать следующей аддитивной формой

$$t_{без\ транз}^{аут} = \sum_{ij \in l_{st,m}^{C}} \frac{1}{\mu_{ij}^{аут}(1-\rho_{ij}^{аут})} + \frac{1}{\mu_{jCA}^{аут}(1-\rho_{jCA}^{аут})} + \frac{1}{\mu_{CAj}^{аут}(1-\rho_{CAj}^{аут})} + \sum_{ji \in l_{st,m}^{C}} \frac{1}{\mu_{ji}^{аут}(1-\rho_{ji}^{аут})} \qquad (11)$$

В предположении, что пакеты трафика аутентификации обслуживаются в сети с одинаковым приоритетом для пакетов данных класса C, то текущее значение коэффициента загрузки *канала* ij трафиком аутентификации $a_{ij}^{аут}$ в общем виде можно представить как

$$\widehat{\rho}_{ij}^{aym} = \frac{L^{aym} + H_{NA}}{L^{aym} - H_{IP}} \frac{Mark_{ij}^{aym} \Theta_{BBU}^{\min}}{V_{ij}} a_{ij}^{aym}, \qquad (12)$$

где $$a_{ij}^{aym} = N_{ij}^{multy} Mark_{ij}^{multy} \lambda_{ij}^{multy} (1 - b^{malty}) \theta_{ij}^{aym} Mn^{aym}. \qquad (13)$$

Здесь θ_{ij}^{aym}, час - непроизводительное время занятия ЛЦТ трафиком безопасности на фазе установления мультимедийного соединения (например, для нашего случая $\theta_{ij}^{aym} = t_{б/з}^{aym}$); Mn^{aym} - математическое ожидание числа служебных сообщений трафика безопасности, приходящихся на один мультимедийный вызов (для нашего примера Mn^{aym}=4); a_{ij}^{aym}, Эрл - трафик аутентификации, порождаемый в сети потоком мультимедийных вызовов при подтверждении взаимной подлинности отправителя и получателя (peer-to-peer authentication).

ПОЯСНЕНИЯ

Текущее значение $\widehat{\rho}_{ij}^{aym}$ ***можно вычислить следующим образом. Пропущенная суммарная изохронная нагрузка в канале*** $ij \in l_{st,m}^{B}$***, полученная для заданной системы маршрутов*** R_{st}^{B} ***в сети, равна*** $\widehat{a}_{ij}^{B} = a_{ij}^{B}(1 - b_{ij}) = \sum_{st \in S^{B,q}} \sum_{m=1}^{M_{st}^{B}} p_{st,m}^{B} \widehat{a}_{st}^{B}$ ***(Эрл). Тогда эффективная скорость передачи, например, трафика аутентификации в канале*** $ij \in l_{st,m}^{C}$ ***определяется соответственно как***

$$V_{ij}^{aym} = \upsilon^{aym} \widehat{a}_{ij}^{aym}, \quad \textbf{???? или} = V_{ij} \widehat{a}_{ij}^{aym} \qquad \textbf{(3.7)}$$

С другой стороны требуемая минимальная эффективная скорость переноса речевого трафика в канале $ij \in l_{st,m}^{C}$ ***вычисляется через общий критерий эффективности*** K_{ij}^{aym}***:***

$$V_{ij}^{aym} = V_{ij} K_{ij}^{aym} = V_{ij} \frac{(L^{Bp} - H_{IP}) \widehat{\rho}_{ij}^{aym}}{L^{Bp} + H_{NA}}. \qquad \textbf{(3.8)}$$

Приравнивая (3.7) и (3.8) и разрешив уравнение относительно ρ_{ij}^{Bp}***, получаем удельную загрузку системы речевым трафиком***

$$\widehat{\rho}_{ij}^{aym} = \frac{L^{Ba} + H_{NA}}{L^{Ba} - H_{IP}} \frac{\upsilon^{aym}}{V_{ij}} \widehat{a}_{ij}^{aym}, \qquad \textbf{(3.9)}$$

Ясно, что должно выполняться неравенство

$$\frac{L^{Ba} + H_{NA}}{L^{Ba} - H_{IP}} \frac{\upsilon^{aym}}{V_{ij}} \widehat{a}_{ij}^{aym} \le \rho_{ij}^{aym\max}, \qquad \textbf{(3.10)}$$

Текущая загрузка ЛЦТ базовыми потоками ρ_{ij}^{B} ***и*** ρ_{ij}^{C} ***в МСС на технологии IP-QoS с учетом абсолютного приоритета обслуживания речевых пакетов (с дообслуживанием) по отношению к пакетам данных дается выражениями [19]***

$$\rho_{ij}^{B} = \frac{L^{B} + H_{NA}}{L^{B} - H_{IP}} \frac{Mark_{ij}^{B}\Theta_{BBU}^{\min}}{V_{ij}} \hat{a}_{ij}^{multy} \eta^{B} z^{B}, \qquad (20)$$

С учетом трафика безопасности среднее время T_{ij}^{*C} ***пребывания пакета в ЛЦТ дается следующим выражением [19]:***

$$T_{ij}^{*C} = \frac{1}{\mu_{ij}^{C}} + \frac{\frac{\lambda_{ij}^{C}}{(\mu_{ij}^{C})^{2}} + \frac{\lambda_{ij}^{aym}}{(\mu_{ij}^{aym})^{2}} + \frac{\lambda_{ij}^{B}}{(\mu_{ij}^{B})^{2}}}{(1-\rho_{ij}^{B}-\rho_{ij}^{C}-\rho_{ij}^{aym})} + \rho_{ij}^{B} T_{ij}^{C}.$$

$$\rho_{ij}^{C} = 1-\rho_{ij}^{B} - \frac{L^{C} + H_{NA}}{T_{ij}^{C} V_{ij}} - \frac{\rho_{ij}^{B}}{1-\rho_{ij}^{B}} \frac{L^{B} + H_{NA}}{T_{ij}^{C} V_{ij}}. \qquad (21)$$

Здесь H_{NA} ***- заголовок уровневого примитива уровня сетевого доступа, бит;*** η^{B}, z^{B} ***- соответственно коэффициенты уплотнения пауз в речевом потоке и коэффициент сжатия речевого потока;*** T_{ij}^{C} ***- заданное среднее время пребывания пакета данных в ЛЦТ, с.***

При сделанных выше предположениях суммарный коэффициент загрузки ЛЦТ трафиком данных и трафиком безопасности будет иметь следующий вид

$$\rho_{ij}^{*C} = \rho_{ij}^{C} + \rho_{ij}^{aym},$$

$$V_{ij}^{Bp\min} = V_{ij} K_{ij}^{Bp} = V_{ij} \frac{L^{Bp} - H_{IP}}{L^{Bp} + H_{NA}} \rho_{ij}^{Bp}, \qquad (3.20)$$

$$V_{ij}^{Cp\min} = V_{ij} K_{ij}^{Cp} = V_{ij} \frac{L^{Cp} - H_{IP}}{L^{Cp} + H_{NA}} \left(1 - \rho_{ij}^{Bp} - \frac{L^{Cp} + H_{NA}}{V_{ij} T_{ij}^{Cp}} + \frac{\rho_{ij}^{Bp}}{1-\rho_{ij}^{Bp}} \frac{L^{Bp} + H_{NA}}{V_{ij} T_{ij}^{Cp}}\right). \qquad (3.21)$$

$$T_{st}^{Cp} = \sum_{m=1}^{M_{st}^{C}} p_{st,m}^{Cp} \; T_{st,m}^{Cp} - \frac{L^{Cp} - H_{IP}}{\omega^{C}} = \sum_{m=1}^{M_{st}^{C}} p_{st,m}^{Cp} \left(\sum_{ij \in I_{st,m}^{C}} T_{ij}^{Cp} + \sum_{\forall i : ij \in I_{st,m}^{C}} T_{i}^{Cp}\right) - \frac{L^{Cp} - H_{IP}}{\omega^{C}} \le T^{Cp}.$$

Формализация фазы авторизации отправителя (пользователя) на сервере инфоуслуг

Авторизация отправителя данных или контроль доступа на серверах инфоуслуг соответствующих поставщиков в сети используется для определения его полномочий на установление сеанса связи с целью использования разрешенных ресурсов в сеансе связи. При этом механизмы контроля доступа могут быть задействованы как в процессе формирования сигнального сообщения, так и на транзитных узлах сети маршрута его прохождения.

Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам — объектам. В качестве субъектов в простейшем случае понимается пользователь. Механизмы контроля доступа - это механизмы, которые используются для усиления стратегии ограничения доступа к ресурсу за счет доступа к нему только тех пользователей, которые имеют на это полномочия. Технология включает использование списков или матриц контроля доступа (которые обычно содержат идентификационные данные контролируемых элементов и санкционированных

пользователей, например, лиц или процессов) в информационной базе контроля доступа (ИБКД), которая определяет права доступа к ресурсам системы (объектам) для отдельных субъектов доступа; аутентифицирующей информации, например, паролей; возможностей, меток или признаков, обладание которыми будет использовано для подтверждения прав доступа и др.

Модель механизмов обеспечения контроля доступа строится как многофазная СМОУб проверки полномочий субъекта [22,23], и включает в себя процесс передачи (пароль, метка защиты) $t^{P}_{ij,прд}$ ***и процесс обработки предъявленных полномочий*** $t^{P}_{j,авт}$ ***(проверка пароля, метки защиты, списков прав доступа) и может быть представлена в виде***

а) $t_{контр\_дост} = t^{P}_{ij,прд} + t^{P}_{j,авт}$ ***– без использования ИБКД;***

б) $t_{контр\_дост} = 2\, t^{ИБКД}_{j,ИБКД\,прд} + t^{ИБКД}_{j,авт}$ ***– с использованием ИБКД.*** ***(26)***

Кроме того, при использовании политики доступа на основе правил может быть задействован механизм управления маршрутизацией.

В [23] описан диспетчер доступа к сетевым ресурсам, приводится оценка влияниия, оказываемая на вычислитиельную систему системой защиты, в качестве которой выступает система разграничения доступа к ресурсам файловой системы и реестра с учетом «ПРОЦЕССА» как самостоятельного субъекта доступа. Предложена формула для расчета трудоемкости алгоритма анализа запроса доступа к ресурсу, а также среднего времени обслуживания в СМО «Система защиты». Делается вывод, что эффективность использования вычислительного ресурса при реализации механизма управления доступом к ресурсам незначительно зависит от используемых приложений (типа используемого приложения) при этом влияние на загрузку вычислительной системы пропорционально количеству решаемых задач и обратно пропорционально трудоемкости задачи. Поэтому наибольшее влияние в данном случае оказывается при загрузке системы задачами с низкой трудоемкостью этапа счета и большим количеством обращений к ресурсам при выполнении задачи.

Постановка задачи проектирования системы сигнализации МСС

????Величины $t^{kRSBP}_{st}\left(\left\{ p^{k}_{st,m} \right\}, \left\{ V_{ij} \right\}\right) \geq \theta^{k}_{st,m}$)

или $\Pr^{k}_{st}\left\{ t^{kRSVP}_{st,m} \geq \theta^{k}_{st,m} \right\} \equiv \Pr^{k}_{st}(t^{kRSBP}_{st}\left(\left\{ p^{k}_{st,m} \right\}, \left\{ V_{ij} \right\}\right) \geq \theta^{k}_{st,m})$ **(15)**

для $\forall\ st \in S^{k}$ **как функция системы глобальных вероятностей маршрутизации** $\left\{ p^{k}_{st,m} \right\}$ **и системы пропускных способностей** $\left\{ V_{ij} \right\}$ **является основой для проектирования (оптимизации) сети сигнализации МСС.**